Available online at www.sciencedirect.com

SCIENCE DIRECT®

ELSEVIER

Annals of Pure and Applied Logic 137 (2006) 317–359

ANNALS OF PURE AND APPLIED LOGIC

www.elsevier.com/locate/apal

Formal Zariski topology: Positivity and points ☆

Peter Schuster

Mathematisches Institut, Universität München, Theresienstraße 39, 80333 München, Germany

Available online 20 June 2005

Abstract

The topic of this article is the formal topology abstracted from the Zariski spectrum of a commutative ring. After recollecting the fundamental concepts of a basic open and a covering relation, we study some candidates for positivity. In particular, we present a coinductively generated positivity relation. We further show that, constructively, the formal Zariski topology cannot have enough points.

Keywords: Commutative ring; Zariski spectrum; Formal topology; Positivity relation; Coinductive generation; Formal point

1. Introduction

The prime spectrum of a commutative ring is a space whose points are the prime ideals of this ring. Rooted in the 19th century German school of what today is called algebraic number theory, the concept of a prime ideal is literally of idealistic origin. To achieve the uniqueness of prime factorisation—which is folklore for the rational integers—also for the ring of integral elements of an arbitrary algebraic number field, Kummer imaginarily extended any such ring by 'ideal numbers' that allow for a unique factorisation as products of

☆ This article is based on the first part of the author's *Habilitationsschrift* [P.M. Schuster, Spectra and Sheaves in Formal Topology, Habilitationsschrift, Universität München, 2003], whose second part, on the Zariski spectrum as a formal geometry, will be published separately [P.M. Schuster, The Zariski spectrum as a formal geometry (forthcoming)].

E-mail address: Peter.Schuster@mathematik.uni-muenchen.de.

0168-0072/$ - see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.apal.2005.05.026

‘ideal prime numbers’. This idea was then realised by Dedekind, who introduced the ideal (prime) numbers just as the (prime) ideals of those rings of integers [42, Ch. 1, Section 3].

Prime ideals are typical points inasmuch as many of them—more specifically, certain maximal polynomial ideals[1]—can be viewed as that which has been made out of the points in geometry during the algebraisation process that Descartes started with representing points by coordinates. One may thus interpret the concept of a prime ideal as a late successor of Euclid’s likewise idealistic definition of a point as an object with no parts or, in modern terms, with no extension.

To estimate properly the major role played by the prime spectra of commutative rings, one should take into account that each scheme—the modern adaptation of the classic notion of an algebraic variety lying right at the basis of algebraic geometry—can be covered by open subschemes each of which is an affine scheme: that is, isomorphic to a prime spectrum. This property, moreover, is characteristic of schemes, just as being locally homeomorphic to an open subset of a Euclidean space is characteristic of differentiable manifolds.

Algebraic geometry as summarised in [25] was given its current form in the second half of the 20th century, mainly by the French group around Grothendieck and Serre. They departed from the work of Chow, Weil, Zariski, and others, who translated the vivid achievements of the Italian school of geometers (Castelnuovo, Enriques, Severi, et al.) to the language of modern algebra. This was started in the meantime by Hilbert, Krull, Emmy Noether, and their followers—and evolved around the concept of an ideal.

As today’s algebraic geometry has led to a proof of Fermat’s conjecture, its power is beyond doubt. The concept of a scheme allows for using geometric methods in algebraic number theory, whereas the previous notion of a variety was too narrow for such purposes.[2] The price one has to pay for the strength of contemporary algebraic geometry is, in addition to the relatively high degree of abstractness, its nonconstructive and impredicative character, which to some extent originates in the idealistic nature of prime ideals.

Besides causing reservations from a foundational perspective, this drawback has yet prevented algebraic geometry from any wholesale formulation in a mathematical theory that is more akin to a high-level programming language than it is the traditional one. Now, however, the time seems ripe for re-approaching this area in such a way that the requirements of those theories are met as perfectly as possible.

By beginning such an approach, we want to prepare that field for the eventual computer-assisted treatment by means of appropriate proof-developing systems. To mention only a few of them (in alphabetical order), there are Agda/Alf(a), Coq, Isabelle, Lego, Minlog, and Nuprl, of which the first is allegedly best suited for handling formal topology: it is explicitly based on predicative Martin-Löf type theory, and the formalisation of proofs from formal topology has already begun [13,11].

In contrast to computational algebraic geometry based on the concept of a Gröbner basis (see, for example, [17]), the object of our undertaking is to provide a universal

1 For more details, see Footnote 7.

2 See [42, Ch. 1, Section 13, Section 14] for a fairly elementary explanation why the theory of schemes is the canonical transit area between number theory and algebraic geometry.

formalisation, as close as possible to the received setting, which not only facilitates machine-supported reasoning but also the extraction of programs from proofs. We aim at theorems whose proofs can be checked by routines within the theory, so that every program taken from a formalised proof is provably correct: the original proof serves also as a correctness proof.

Rather than developing a separate algorithm for each existence theorem, we want to modify the given theory so that the essence of the program is already present in the proof. Although safety has then priority over feasibility, nothing hinders one from carefully tuning the algorithms later. In this context, one also ought to take into account that secure software has become a more relevant issue, and that developing programs by ad hoc means might later be regarded as a waste of human resources.

In addition to dispensing with termination proofs that make use of metatheoretical suppositions such as the validity of proofs by contradiction, we avoid any assumption that might conflict with a computational model, or even with an actual implementation, of the algebraic structures under consideration. In particular, we do not assume the decidability of equality, let alone the stronger one of subset membership. Our motivation for not assuming even the former is that we want to cope equally with algebraic geometry over the real or complex numbers, rather than unnecessarily restricting our attention to the case of discrete base fields.

In algorithmic algebraic number theory, on the other hand, it is legitimate to assume 'that there is a clear-cut answer whether a is equal to b or whether a, b are distinct' [45, p. 6]; indeed, this provably holds for algebraic numbers [38, Theorem VI.1.9]. To decide which alternative holds in a specific instance may nonetheless require considerable computational efforts; whence one better avoids building one's theory upon assumptions like this.[3]

It is anyway little clear whether one may suppose the decidability of the membership of the ideal I of $\mathbb{Z}$ that is generated by the perfect numbers: as 1 belongs to this ideal if and only if there exists an odd perfect number, any such decidability assumption would lead to a too simple solution of the open problem of whether there actually is an odd perfect number. In particular, we cannot say yet whether $1 = 0$ in the quotient ring $\mathbb{Z}/I$.

By following the lines of Bishop-style constructive algebra [6,38], we expect to end up with a theory that is suited as the core of all more technical settings, just as constructive analysis serves for a theoretical basis of computational and recursive analysis [7,5]. A further feature of our approach is that the geometry is kept closer to the underlying algebra; whence a widespread attitude will once more be disproved: that any attempt to avoid the putative short cuts somewhat peculiar to classical mathematics—which in effect often destroy some of the information contained in the initial data—inevitably involves unwelcome complexity.

Enough evidence of the practicability of this project is already provided by an alternative treatment of the Zariski topology on the prime spectrum of a commutative ring with unit. This attempt requires us to regard points—that is, in this case, prime ideals—as truly ideal entities, a strategy which is one of the characteristics of formal topology. We therefore decided to work within this theory, which was put forward in the mid 1980s by Giovanni

3 We owe this argument to Jesper Carlström.

Sambin [47] in order to make available to Martin-Löf type theory [36] the concepts of classical topology that are worth keeping to such a constructive and predicative framework.

As since raised by, among others, the Padua, Gothenburg, and Uppsala schools of mathematical logic, formal topology has proved a fairly universal setting for doing topology in a point-free way; we refer to [49] for a recent and exhaustive overview. It has successfully been applied in various areas of pure mathematics, symbolic logic, and theoretical computer science, and simultaneously generalises locale theory and domain theory [53,48,41].

In return, we supply, as a by-product of our work, a variety of algebraic–geometric examples suited for the future study of formal topology. Note, moreover, that the concept of a spectral locale, which is the point-free counterpart of Hochster's notion of a spectral space [26], is crucial for non-Hausdorff point-free topology in general, and for its applications in domain theory in particular [61, Ch. 9]. As being a spectral space means to possess the characteristic properties of the spectrum of a commutative ring, we even provide examples of *spectral* formal topologies in a sense yet to be made precise.

A further task of our studies, which we perform in [55], is to indicate that a concept of a sheaf on an arbitrary formal topology can be abstracted in a fairly canonical manner from the formal adaptation of the structure sheaf on the Zariski spectrum. Since Leray and Henri Cartan introduced the language of sheaves in the years after World War II, it has clearly been an indispensable tool for geometry, topology, and related disciplines. Later on, sheaves gave rise to topos theory (see [33] for an introduction), a fairly subtle construct which is often proposed as a categorical foundation for mathematics.

From a constructive standpoint, topos theory is fine as a foundation in so far as the natural logic for topos theory is the intuitionistic one,[4] and it dispenses with all forms of the axiom of choice. From a predicative perspective, however, topos theory causes some worries about its peculiarly unrestricted use of the full power set. More specifically, set comprehension and related principles are constructively incompatible with choice principles: in the presence of a sufficiently strong version of either, the law of excluded middle can be deduced [19,24].

Also Martin-Löf type theory, which as yet includes a fairly general choice principle [36, pp. 50–2], may get infected with classical logic as soon as one relaxes the regulations for how to form sets. Rather strong power set and effective quotient constructors were looked at in this context [34,35]. There is nonetheless a promising avenue to connect topos theory with type theory: the so-called logic-enriched type theory [1] is an extension of Martin-Löf type theory which allows us to do without the proposition-as-types interpretation, and thus without the type-theoretic choice principle.[5] Among other things, our work is intended to complement this approach; perhaps the formal variant of sheaves we propose in [55] will eventually serve as the starting point of an alternative and perhaps easier path to topos theory.

4 This is intuitively clear when one takes into account that the open subsets of a topological space usually form a Heyting algebra rather than a Boolean algebra: the complement of an open set is seldom open, too, and the pseudo-complement (that is, the interior of the complement) is not a true complement.

5 Milly Maietti and Nicola Gambino explained this to us with patience.

Since formal topology can now be seen as a more and more independent offspring of type theory, we may use it as a mathematical theory per se. In particular, we do not follow every conceptual distinction peculiar to type theory, let alone all its notational conventions, but are confident that most of them can be imposed without major difficulties as occasion demands. One could simply say that we are doing formal topology informally.

2. Points versus opens

Grothendieck and others[6] solved the representation problem

> *for each commutative ring A with unit, find a topological space and a sheaf of local rings on it such that A is the ring of global sections of this sheaf*

by equipping the prime spectrum

$$\mathrm{Spec}(A) = \{\mathfrak{p} \subset A : \mathfrak{p} \text{ prime ideal of } A\}$$

of A with the Zariski topology,[7] and this with the so-called structure sheaf. In spite of the defects this classic solution shows from a critical perspective (see below), it possesses a considerable constructive content—to be revealed during the course of this article and its follower [55]—which still allows for a topological representation of commutative rings, and even for an appropriate adaptation of the well-known universal property of $\mathrm{Spec}(A)$ as a locally ringed space together with that structure sheaf.

At least three features of the Zariski topology on $\mathrm{Spec}(A)$ attract our attention. First, the canonical basis of open subsets

$$D(a) = \{\mathfrak{p} \in \mathrm{Spec}(A) : a \in A \setminus \mathfrak{p}\} \qquad (a \in A)$$

is a family whose index set coincides with the given ring A. Secondly,

$$D(1) = \mathrm{Spec}(A)\,,$$

6 We refer to [28, p. 222] for a historical overview.

7 Classically speaking (as frequently throughout this footnote), the Zariski topology on $\mathrm{Spec}(A)$ is given by prescribing its closed subsets as those of the form

$$Z(\mathfrak{a}) = \{\mathfrak{p} \in \mathrm{Spec}(A) : \mathfrak{a} \subset \mathfrak{p}\}$$

with $\mathfrak{a}$ being an ideal of A. This definition is grounded in the concrete Zariski topology on $\mathbb{C}^n$, say, whose closed subsets are just the algebraic varieties

$$Z(\mathfrak{a}) = \left\{z \in \mathbb{C}^n : f_1(z) = \ldots = f_m(z) = 0\right\}.$$

Here $\mathfrak{a}$ is an ideal of $A = \mathbb{C}[X_1, \ldots, X_n]$, which, by the Hilbert basis theorem, is generated by finitely many polynomials $f_1, \ldots, f_m$. Needless to say, the Zariski topology on $\mathbb{C}^n$ is coarser than the norm topology.

By the Hilbert Nullstellensatz, moreover, the maximal ideals of this particular polynomial ring A are just the ideals that are generated by n monic linear polynomials $X_1 - z_1, \ldots, X_n - z_n$, and thus correspond precisely to the points $(z_1, \ldots, z_n)$ of $\mathbb{C}^n$. In addition to these closed points, $\mathrm{Spec}(A)$ contains, among the various other prime ideals of A, the zero ideal as a dense point—its so-called generic point. As every nonempty open subset of $\mathrm{Spec}(A)$ contains this generic point, Zariski topologies are in general not T_1, whereas they are readily seen to be T_0; moreover, they are spectral, and thus sober.

which is to say that the unit of A is an index for the entire space. Thirdly,

$$D(ab) = D(a) \cap D(b)$$

for all $a, b \in A$; in other words, the intersection of basic open sets corresponds on the index level to nothing but the multiplication in A.

This situation mirrors the idea underlying formal topology almost as perfectly as if formal topology was originally tailored for dealing with the Zariski topology (which, of course, it was not, at least not exclusively, but compare the paradigmatic character of spectral spaces indicated before). For reasons that will be explained in a moment, it indeed appears fairly natural to cast the points of $\mathrm{Spec}(A)$ in a secondary role, and, moreover, to take seriously the fact that the indices of the basic open sets—that is, the elements of A—are the primitive objects.

The essence of formal topology now is to adopt such a shift of perspective as a general principle. More specifically, the received conceptual precedence of points over open sets is completely reverted, and, secondly, the role of a basis of the topology is played by any monoid whatsoever, which mostly is supposed to be commutative. In the same way in which the multiplicative monoid of a commutative ring A represents the basis of the Zariski topology on $\mathrm{Spec}(A)$, in a formal topology the monoid operation stands for the intersection of the members of the basis, and the unit of the monoid for the entire space.

In general, a basis of a topological space neither is closed under intersection nor includes the whole space. Likewise, the concept of a formal topology as based on a monoid—or, more specifically, on a meet-semilattice [47]—does not serve for all purposes; whence today formal topology usually comes without monoid structure [49]. In the present context of formal Zariski topology we may stick to the former setting, with a multiplicative operation on the basis being given, and mention the latter approach only in passing.

The elements of the monoid of a formal topology are called *basic opens*, just because they are thought to represent the basic open sets, whereas the concept of an arbitrary open set is substituted by that of an *arbitrary open*. The latter means a subset[8] of the given monoid, which is intended to stand for the union of all the basic open sets whose indices are elements of this subset—and therefore indeed represents an arbitrary open set. In this vein, one uses the letters $U, V, W, \ldots$, which traditionally stand for open subsets, to denote arbitrary opens, whereas $a, b, c, \ldots$ are chosen as symbols for basic opens.

The notion of a formal point enters the stage of formal topology only, if at all, in a late act, as a subset of the monoid that behaves as if it would consist of the indices of a neighbourhood filter of an imagined point. Every topological space in the usual sense, with an underlying set of points, gives rise to a formal topology, and each of its points defines a formal point. What, however, is wrong with starting from points?

On the one hand, the concept of a point looks vague, if not void, from the constructive standpoint, and this particularly applies to the case of the Zariski spectrum. So the classical

[8] We thus deviate from some of the literature on formal topology where an arbitrary subset of the monoid is already called a formal open, and reserve this notion for subsets that are saturated with respect to the covering. The wider use of this term is in compliance with tacitly identifying any subset with its saturation, a strategy which we do not follow either. We also refer to [43] for an extension of Martin-Löf type theory with a concept of a subset, and to [52,10] for interpretations of subsets within type theory.

notion of a prime ideal is constructively too restrictive: in general, one may hardly find any point in $\mathrm{Spec}(A)$. For instance, not even the zero ideal in the sufficiently concrete fields of real or complex numbers can constructively be thought of as a prime ideal, as we shall recall in Section 3.

In the presence of the axiom of dependent choices, the existence of a maximal or prime ideal in a nontrivial countable ring is equivalent to LPO and LLPO, respectively [31], which are fragments of the law of the excluded middle (see Section 3). The existence of a maximal or prime ideal in an arbitrary nontrivial commutative ring is equivalent—at least classically—to the full axiom of choice or the Boolean ultrafilter theorem, respectively (see [2] for an overview).[9] Accordingly, the Zariski spectrum may fail to have enough points within a general topos which lacks the appropriate variant of the axiom of choice [27, p. 258], of which there are plenty. As Zorn's lemma is traditionally used for 'constructing' a maximal ideal in a nontrivial ring, it should be clear that any such 'construction' is not a construction in the true sense of the word, but rather postulates the existence of an ideal object on the mere grounds of an actually given coherent method to approximate it by real objects.[10]

The more or less doubtful ontological status of prime ideals is of particular relevance when one wishes to employ one of the local–global principles, frequently occurring in commutative algebra and algebraic geometry, by which a certain 'global' property (of a ring, module, homomorphism, etc.) is reduced to the whole of 'local' versions of this property that are achieved by localising the objects under consideration at every prime ideal of the underlying ring. In any such way, one risks accepting the conjunction of a family indexed by a possibly empty set as a defining or sufficient condition for the property in question, no matter whether the latter really is a tautology.

With sheaves of local rings together with the appropriate concept of morphisms between locally ringed spaces, we encounter in [55] a few characteristic examples for defining a property by passing from the local to the global. However, we also see in [55] how to handle these definitions in a truly local, point-free manner—the traditional method, involving prime ideals, may better be called 'pointwise' rather than 'local' anyway. We further refer to [32] for constructive local–global principles neither involving prime nor maximal ideals but still suited for proving such famous theorems as the ones of Horrocks and Quillen–Suslin, and the Serre conjecture.

Anybody with a certain knowledge of intuitionistic algebra [46,59], locale theory [28, V.3.2], or topos theory [39,58][11] might argue that the notion of a prime ideal should

[9] From a classical perspective, one might argue that most rings occurring in algebraic geometry, say, are finitely generated algebras over a field (that is, quotient rings of polynomial rings in finitely many variables) and thus, by Hilbert's basis theorem, satisfy the ascending chain condition for ideals; whence the existence of a maximal ideal in every nontrivial ring of this kind can be proved without invoking the axiom of choice. This argument, however, works only classically, because constructively one can at most expect that, in a finitely generated algebra over a discrete field, in each ascending chain of ideals two successive elements coincide, rather than all but finitely many of them. For a more detailed discussion thereof see [38, VIII.1]; we wish to thank Fred Richman who has reminded us thereof.

[10] There is some evidence for that a certain understanding of Zorn's lemma is more harmless than the axiom of choice [4], but this understanding hardly suffices for 'constructing' maximal ideals in general.

[11] We are grateful to Steve Vickers for these references.

anyway be replaced by that which is synonymously known as a prime coideal, prime anti-ideal, or prime filter. This positively describes the properties characteristic of the complement of a prime ideal, and 'because it is at these objects that we wish to localize, and since $\neg\neg \neq id$, we must deal with them directly' [58, p. 194]. Indeed, the real or complex numbers different from zero form a prime filter; more generally, so do the invertible elements of every nontrivial local ring.

All their virtues notwithstanding, prime filters are not really an alternative: except for the aforementioned and a few other relatively simple cases (see [46] and [59, Ch. 8]), they seem to be even harder to grasp than prime ideals. As for the latter, there appears to be no universal existence proof for the former that can do without any principle related to the axiom of choice, and up to now the intention of effectively presenting coideals reduces this concept to that of a complement of a finitely generated or even principal ideal.

Besides, the prime filters of a commutative ring A turn out to be the formal points of the formal Zariski topology of A, with their truly idealistic character. As shown in [55], one even cannot expect to prove constructively that the formal Zariski topology of an arbitrary discrete ring has enough (formal) points in a sense analogous to the one of locale theory [20].[12] Since, however, coideals in general will play a central role in the subsequent development of our theory, we shall undertake a successful attempt to coinductively generate a family of coideals that is essential for completing the so-called basic picture of Zariski topology (Section 6.1).

On the other hand, the open sets of a topological space are usually formed as collections of elements of the underlying set, by invoking principles of classical set theory which may already cause foundational doubts. In any such case, moreover, every quantification over open sets necessarily involves a possibly impredicative second-order quantification: namely, over subsets of the set underlying the topological space. To establish open subsets of $\mathrm{Spec}(A)$, by gathering prime ideals together, is even of third order: it means to form sets of subsets of the given set, the ring A—every point of $\mathrm{Spec}(A)$ is, as a prime ideal of A, already a subset of A. Note that literally the same objections apply to prime filters in the place of prime ideals.

Due to the idealistic character of points, it is also no wonder that points must form a higher-order concept; this is already clear from the necessarily infinitary definition of a point on the real line. As various nontrivial topological spaces, the Zariski spectrum may thus have not enough as well as too many points, no matter whether one takes prime ideals or prime filters as such. Moreover, a conjunction of an infinite family of conditions is particularly hard to verify by finite means when it is indexed by entities of a higher-order character, as it is the case for the local–global principles mentioned before in their classical form.

Most of these reservations disappear as soon as one decides to work within the setting of formal topology, where the characteristic of points as ideal objects is taken seriously: the real objects are the indices of the basic open sets, and a formal point is literally a collection of objects each of which could count as a coherent approximation to an imagined concrete point—that is, to one of the ideal objects. Instead of quantifying over all the open sets, moreover, one then adopts as a rule that it usually suffices to quantify only over the basic

[12] Nicola Gambino has kindly pointed out this concept to us.

open sets, and that one can equally do so with their indices: the elements of the given monoid. Needless to say, one thus also meets Ockham's request for the greatest possible conceptual simplicity, at least in cases like the present one in which the indices are much more primitive than the basic open subsets.

The monoid under consideration has, of course, to be granted as a set over whose whole one can legitimately expect complete control. In this vein, we presume throughout that the commutative ring A we deal with behaves well in all relevant respects, a demand which, of course, has to be made precise when required. By focusing on the elements of A as the indices of the basic opens, one also keeps as close as possible to the given data—which, in our example, include the algebraic structure of the commutative ring A. Hence one automatically preserves most of the information contained in these data, and avoids stepping beyond their logical and computational complexity, whereas different point-free approaches to topology fall short of such expectations, at least from our perspective.

For instance, to establish the Zariski spectrum of A as a locale (see [28, V.3] and [61, 12.2]) one starts with the distributive lattice that is generated by the expressions of the form $D(a)$ and equipped with the following relations:

$$\begin{array}{ll} D(1) = 1, & D(ab) = D(a) \wedge D(b), \\ D(0) = 0\,, & D(a+b) \leq D(a) \vee D(b). \end{array} \tag{1}$$

This so-called *reticulation* $L(A)$ of A à la Joyal [30] and Simmons [57] is isomorphic to the distributive lattice of the radicals of finitely generated ideals [14] in the same way in which the ideal completion of $L(A)$ is isomorphic to the coherent frame of all the radical ideals of A [28, V.3.2]. As in [14] the former is called the *Zariski lattice* of A, we may aptly call the latter the *Zariski frame* of A. Note also that the Zariski lattice is nothing but the lattice of compact elements of the Zariski frame.

Apart from perhaps being somewhat unpalatable to some people,[13] any talk of lattices and related concepts (frames, locales, quantales, etc.) looks secondary in the present context, if not somewhat redundant. Formal topology, on the other hand, allows one to do without that language—unless and until one wishes to link the former with areas expressed within the latter. This is best illustrated by the fact that the category of formal topologies becomes equivalent to that of frames as soon as one allows impredicative reasoning [47]; whence a predicative notion of a frame is 'nothing but the notion of a formal topology' [49].

Besides having led to a fairly universal treatment of several lattice-theoretic disciplines [3], formal topology appears to us as a refinement thereof in many respects. We even hold that this particularly applies to the case of the Zariski spectrum, although in [14] the Zariski lattice is said 'to contain all the informations necessary for a constructive development of the abstract theory of the Zariski spectrum'. By passing to radical ideals, namely, one partially loses the multiplicative structure of A, whereas this is completely maintained in the formal Zariski topology.

For the same reason we neither follow [56], where a definition of the Zariski spectrum as a formal space begins with identifying each element of A with all its powers, nor the construction of the corresponding meet-semilattice in [28, V.3.1]. Any such turn would

13 Comprising the author until he has recently learned better.

only make sense as long as one concentrates on the derived topology of the Zariski spectrum, and allows oneself to neglect the original character of A as a commutative ring.

We hesitate to subscribe to this strategy, but have to admit that also in the case of the formal Zariski topology we apparently need to keep extant the additive structure of A, which goal is achieved without any extra effort as a by-product of introducing the structure sheaf also in the formal context [55]. This sheaf of local rings transports the ring structure of A as a whole, and has to adjoin the formal Zariski topology anyway in order to arrive at the universal property thereof [55].

Last but not least, our way to the formal Zariski topology of A is an elementary short cut of the following road. First, by inverting the Scott entailment relation $\vdash$ on A from [12], one again gets an entailment relation $\dashv$ on A; see also [14]. Next, there is the distributive lattice assigned to $\dashv$ in the sense of [12], which happens to coincide with $L(A)$. The frame of ideals of that lattice is then a coherent frame [28, II.3.2]. Finally, the Stone formal topology associated with this coherent frame [47,40] is just the formal Zariski topology of A. Also in comparison with this sophisticated approach, the reader may judge our direct path in the sequel.

3. Rings with inequality

Before entering the context of formal Zariski topology more deeply, we have to collect some concepts peculiar to commutative algebra or to constructive mathematics, or to both [38,46,59].

To start with, recall that a set is *inhabited* if and only if one can present an element of it. We distinguish this notion from the constructively weaker one of being *nonempty*, which only means that the assumption that this set be empty is contradictory.

Following a convenient notation common to formal-topological circles, we say that two subsets S, T of a fixed set *meet* each other, for short $S \between T$, whenever their intersection $S \cap T$ is inhabited. Note that $S \between S$ is equivalent to S being inhabited, and that if $S = \{s\}$, then $S \between T$ amounts to $s \in T$.

We suppose throughout that 0 is not a natural number; in other words, we set $\mathbb{N} = \{1, 2, 3, \ldots\}$, and $\mathbb{N}_0 = \{0\} \cup \mathbb{N}$. We also call a set S *finite* whenever for some $n \in \mathbb{N}_0$ there is a mapping from $\{1, 2, \ldots, n\}$ *onto* S. Every finite set S of this kind is either empty or nonempty depending on whether $n = 0$ or $n \in \mathbb{N}$, respectively.[14]

Every ring A occurring subsequently is assumed to have a unit 1 and to be commutative.[15] As many sets in constructive mathematics, A is to arrive with two binary relations, an equivalence relation $=$ understood as *equality*, and a symmetric relation $\neq$ intended as *inequality* which we assume to be consistent with equality in the sense that

14 This use of the term 'finite set' differs from that in some literature on constructive mathematics. So in [38] a finite set is, in addition, required to be discrete (see below), which is to say that its elements are in a one-to-one correspondence with the numbers $1, \ldots, n$ for some integer $n \geq 0$. Finite sets in our weaker sense are then called 'finitely enumerable'.

15 The attentive reader may excuse that to prepare the noncommutative case we sometimes have chosen a formulation that appears somewhat redundant in the commutative case.

$\neg(a = b \wedge a \neq b)$ for all $a, b \in A$. In particular, each of the statements $a = b$ and $a \neq b$ implies the negation of the other.

However, we do not suppose from the outset that $\neq$ be the *denial inequality* for which $a \neq b$ already if $\neg(a = b)$. This interpretation of $\neq$ as deriving from $=$ is admissible, but it is only one interpretation; another one is to regard $\neq$ as a positive concept relatively independent from $=$ (as for real and complex numbers, see below). Likewise, it is not generally assumed that $\neq$ be *tight*, which is to say that $a = b$ already if $\neg(a \neq b)$, let alone that A is *discrete*—that is, either $a = b$ or else $a \neq b$ for all $a, b \in A$.

In most cases one nonetheless conceives an inequality to be *standard* in the sense of [38]—that is, equivalent to the denial inequality in the presence of classical logic. Note that in classical mathematics one tacitly presupposes A to be discrete with the denial inequality. Among the rings naturally occurring in mathematics, some are perfectly discrete also from the constructive perspective ($\mathbb{Z}$, $\mathbb{Q}$, the field $\mathbb{A}$ of algebraic numbers, polynomial rings over such rings, ...), but some are not: $\mathbb{R}$ and $\mathbb{C}$ do not even come with the denial inequality (see below).

We expect all ring operations, homomorphisms, relations, predicates, subsets, etc. to be *extensional* (that is, to respect equality), but to be *strongly extensional* (that is, to reflect inequality) only whenever so declared. For instance, we require every ring homomorphism $\psi : A \to B$ not only to satisfy $\psi(1) = 1$, but also to be both extensional and strongly extensional: that is,

$$a = b \implies \psi(a) = \psi(b) \quad \text{and} \quad \psi(a) \neq \psi(b) \implies a \neq b\,,$$

respectively, for all $a, b \in A$.

There sometimes is the need to distinguish two types of a *complement* of each $S \subset A$, namely,

$$\begin{aligned} \sim S \; &= \; \{a \in A : \forall b \in S\ (a \neq b)\}\,, \\ \neg\, S \; &= \; \{a \in A : \forall b \in S\ \neg\,(a = b)\}\,. \end{aligned}$$

In particular, $\sim S \subset \neg\, S$ because $\neq$ is consistent, and $\sim S = \neg\, S$ whenever $\neq$ is the denial inequality. As the membership relation is extensional according to our conventions, $a \in \neg\, S$ precisely when $a \notin S$. We also write $T \sim S$ in place of $T \cap (\sim S)$, and—as usual—$T \setminus S$ in place of $T \cap (\neg S)$.

We use A^* as a symbol for the set of *invertible elements* of A, and say that A is *trivial* or *nontrivial* whenever $0 \in A^*$ or $A^* \subset \sim \{0\}$, respectively.[16] Note that if $\neq$ is the denial inequality, then A is nontrivial precisely when it is not trivial.

According to the logical law of *ex falso sequitur quodlibet*, the denial inequality is contained in the *relative inequality* with $a \neq b$ standing for $a = b \Rightarrow 1 = 0$, where 1 and 0 denote the unit and the zero of the ring A. On the other hand, the relative inequality is consistent with equality if and only if it is contained in the denial inequality, which is the

[16] As we do not generally suppose that $ab \neq 0$ implies $a \neq 0$ and $b \neq 0$ (see below), we cannot define a ring to be nontrivial if just $1 \neq 0$.

case precisely when $\neg(1 = 0)$—so, for instance, whenever A is nontrivial. Every ring is trivially nontrivial with respect to the relative inequality.[17]

We say that a ring *A has recognisable nilpotents* whenever

$$\exists n \in \mathbb{N}\ \left(a^n = 0\right)\ \vee\ \forall n \in \mathbb{N}\ \left(a^n \neq 0\right)$$

for each $a \in A$. Classically, of course, every ring has recognisable nilpotents. More specifically, if $\neq$ is the denial inequality, then $\forall n \in \mathbb{N}\ (a^n \neq 0)$ is the negation of $\exists n \in \mathbb{N}\ (a^n = 0)$; whence A has recognisable nilpotents whenever, in addition, one presupposes an appropriate fragment of the law of excluded middle. When A is even discrete, then it suffices to assume that the *limited principle of omniscience (LPO)* be valid, which says that if $(\lambda_n)_{n\in\mathbb{N}}$ is an increasing sequence in $\{0, 1\}$, then

$$\exists n \in \mathbb{N}\ (\lambda_n = 1)\ \vee\ \forall n \in \mathbb{N}\ (\lambda_n = 0)\,.$$

LPO implies the *weak limited principle of omniscience (WLPO)*, which says that if $(\lambda_n)_{n\in\mathbb{N}}$ is an increasing sequence in $\{0, 1\}$, then

$$\neg\forall n \in \mathbb{N}\ (\lambda_n = 0)\ \vee\ \forall n \in \mathbb{N}\,(\lambda_n = 0).$$

For every discrete ring A, WLPO implies that *A has weakly recognisable nilpotents*: that is,

$$\neg\forall n \in \mathbb{N}\ \left(a^n \neq 0\right) \vee\ \forall n \in \mathbb{N}\ \left(a^n \neq 0\right)$$

for each $a \in A$. A consequence of WLPO is the *lesser limited principle of omniscience (LLPO)*, which says that if $(\lambda_n)_{n\in\mathbb{N}}$ is a sequence in $\{0, 1\}$ with $\lambda_n = 1$ for at most one n, then either $\lambda_n = 0$ for all even n or $\lambda_n = 0$ for all odd n.

A weakening of LPO in a different direction is *Markov's principle (MP)*: that is, if $(\lambda_n)_{n\in\mathbb{N}}$ is an increasing sequence in $\{0, 1\}$, then

$$\neg\,\forall n \in \mathbb{N}\ (\lambda_n = 0)\ \implies\ \exists n \in \mathbb{N}\,(\lambda_n = 1).$$

An obvious consequence of MP is that every discrete ring *A has semirecognisable nilpotents*, which is to say that

$$\neg\forall n \in \mathbb{N}\ \left(a^n \neq 0\right)\ \implies\ \exists n \in \mathbb{N}\ \left(a^n = 0\right)$$

for each $a \in A$.

Clearly, LPO is related to the halting problem for Turing machines, and MP represents an unbounded search. Another good reason for not to accept LPO, WLPO, LLPO, and MP as constructive principles is that each of them reflects an allegedly nonconstructive statement about the real or complex numbers. So LPO follows from the assumption that $\mathbb{R}$

[17] The notion of a relative inequality was kindly pointed out to us by Henri Lombardi, who introduced it for doing constructive algebra without negation but with the trivial ring.

or $\mathbb{C}$ is discrete,[18] and MP from the one that they come with the denial inequality, whose decidability entails WLPO. Finally, LLPO is a consequence of

$$ab = 0 \implies a = 0 \vee b = 0$$

for all real or complex numbers a, b, although its classical contrapositive

$$a \neq 0 \wedge b \neq 0 \implies ab \neq 0$$

holds in any field whatsoever.

Note that LPO, WLPO, and MP are tantamount to $P \vee \neg P$, $\neg\neg P \vee \neg P$, and $\neg\neg P \Rightarrow P$, respectively, for every statement P that is *simply existential* [7], which is to say that P is of the form $\exists n \in \mathbb{N}\ (\lambda_n = 1)$ for a certain (without loss of generality, increasing) sequence $(\lambda_n)_{n \in \mathbb{N}}$ in $\{0, 1\}$. In particular, LPO is equivalent to the conjunction of MP and WLPO. Likewise, LLPO amounts to $\neg\,(P \wedge Q) \Rightarrow \neg P \vee \neg Q$ for simply existential statements P, Q. See, for instance, [7,38] for more details.

Any talk of inequality aside, recall that a subset S of A is an *ideal* whenever

$$\begin{array}{rcl} a = 0 & \implies & a \in S \\ a \in S \wedge b \in S & \implies & a + b \in S \\ a \in S \vee b \in S & \implies & ab \in S \end{array}$$

for all $a, b \in A$, and a *radical ideal* if, in addition,

$$\exists n \in \mathbb{N}\,(a^n \in S) \implies a \in S$$

for all $a \in A$. An arbitrary intersection of (radical) ideals is a (radical) ideal. If we set

$$I\,(b_1, \ldots, b_m) = Ab_1 + \cdots + Ab_m$$

for $b_1, \ldots, b_m \in A$ and $m \in \mathbb{N}_0$, then

$$I(U) = \bigcup \{I\,(b_1, \ldots, b_m) : b_1, \ldots, b_m \in U\,,\ \ m \in \mathbb{N}_0\} \tag{2}$$

is the ideal generated by $U \subset A$. If I is an ideal, then the *radical* of I

$$\sqrt{I} = \left\{a \in A : \exists n \in \mathbb{N}\ \left(a^n \in I\right)\right\}$$

is a radical ideal, and so is

$$R(U) = \sqrt{I(U)} \tag{3}$$

for every $U \subset A$. As for I, we write $R\,(b_1, \ldots, b_m)$ in place of $R\,(\{b_1, \ldots, b_m\})$. Note that $I\,(U) \subset R\,(U)$, and that U is inhabited whenever either $I\,(U)$ has a non-zero element, or $R\,(U)$ has an element all of whose powers are not equal to 0.[19]

The following fairly trivial observation is sometimes useful.

---

18 In the presence of a weak form of countable choice [8] that is valid under classical logic without any choice, LPO is even equivalent to this assumption. The analogous facts hold in the sequel for WLPO, LLPO, and MP.

19 We have chosen not to use the traditional notation (U) and $\sqrt{(U)}$ for the ideal generated by any $U \subset A$ and the radical thereof, respectively: as they lack the dual versions that will be needed later, one may introduce new notations anyway.

Lemma 1. *Let A be a commutative ring and $b_1, \ldots, b_m \in A$. If $a \in I(b_1, \ldots, b_m)$, then for every $k \in \mathbb{N}$ there is $n \in \mathbb{N}$ so that $a^n \in I\left(b_1^k, \ldots, b_m^k\right)$; moreover, each n with $n \geq mk$ will suffice.*

Proof. Let $n \in \mathbb{N}$ be arbitrary, and assume that $a \in I(b_1, \ldots, b_m)$. Then a^n is a linear combination of monomials $b_1^{k_1} \cdot \ldots \cdot b_m^{k_m}$ with $k_i \geq 0$ for every i and $k_1 + \cdots + k_m = n$. So if $n \geq mk$, then—for each of these monomials—$k_i \geq k$ for some $i \leq m$, because if $k_i < k$ for all $i \leq m$, then $k_1 + \cdots + k_m < mk \leq n$, which is impossible. □

We also need to characterise radical ideals in a less usual way.

Lemma 2. *A subset S of a commutative ring A is a radical ideal if and only if*

$$U \subset S \implies R(U) \subset S \tag{4}$$

for all (finite) $U \subset A$.

Proof. Suppose first that S is a radical ideal, and let $a \in R(U)$: that is, $a^n \in I(U)$ for some $n \in \mathbb{N}$. If $U \subset S$, then $I(U) \subset S$; whence $a^n \in S$, and thus $a \in S$. As for the converse, assume that (4) holds for all finite U. Note that $0 \in S$ is the special case $U = \emptyset$ of (4), and let $a, b \in A$. If $a \in S$ or $b \in S$, then $ab \in S$ because $ab \in I(a) \cap I(b)$; if $a, b \in S$, then $a + b \in S$ because $a + b \in I(a, b)$. Finally, if $a^n \in S$, then $a \in S$ because $a \in R(a^n)$. So S is a radical ideal. □

If I is an ideal of a discrete ring A, and one equips A/I with the usual equality of equivalence modulo I and with the corresponding denial inequality, then A/I is discrete precisely when I is a *detachable* subset of A: that is, either $a \in I$ or else $a \notin I$ for each $a \in A$. We do not presuppose that every ideal in a discrete ring be detachable, although so is every principal ideal of $\mathbb{Z}$. For instance, the ideal of $\mathbb{Z}$ that is generated by the perfect numbers is can hardly be expected to be detachable constructively (see Section 1), let alone principal.

A ring A is a *field* whenever $\sim \{0\} = A^*$, an *integral domain* whenever A is nontrivial and

$$a \neq 0 \wedge b \neq 0 \implies ab \neq 0,$$

and a *reduced ring* if

$$a \neq 0 \implies \forall n \in \mathbb{N}\left(a^n \neq 0\right).$$

Every field is an integral domain, and every integral domain is a reduced ring.[20]

In [6], an inequality $\neq$ on a ring A is called a *ring inequality* whenever $\neq$ is *translation invariant* (that is, $a \neq b$ is equivalent to $a - b \neq 0$), and the multiplication in A is strongly extensional with respect to $\neq$, which is to say that

$$ab \neq 0 \implies a \neq 0 \wedge b \neq 0.$$

[20] Our concepts of field and integral domain contain the ones used in [38], with which they coincide whenever $\neq$ is translation invariant and—in the case of integral domains—tight. In [59], however, $\neq$ is generally assumed to be a ring apartness.

On the other hand, $\neq$ is *cotransitive*[21] if $+$ is strongly extensional with respect to $\neq$: that is,

$$a + b \neq 0 \implies a \neq 0 \vee b \neq 0\,.$$

Note that the denial and the relative inequality always are (not necessarily cotransitive) ring inequalities. A tight and cotransitive ring equality is a *ring apartness*. If A is discrete, then $\neq$ is a ring apartness coinciding with the denial inequality. A field with a ring apartness is a *Heyting field*; in addition to all discrete fields, also $\mathbb{R}$ and $\mathbb{C}$ are Heyting fields.

An ideal S of the commutative ring A is a *prime ideal* whenever

$$\begin{array}{rcl} ab \in S & \implies & a \in S \vee b \in S \\ a \in S & \implies & \neg\,(a = 1) \end{array}$$

for all $a, b \in A$. Of course, the principal ideal (p) of $\mathbb{Z}$ that is generated by a prime number p is a prime ideal, and so is $\{0\} \subset \mathbb{Z}$. While every prime ideal is a radical ideal, the former notion is constructively too narrow: that the zero ideal in $\mathbb{R}$ or $\mathbb{C}$ is prime amounts to accept LLPO (see above), whereas $\{0\}$ is a radical ideal in each of these Heyting fields.

Each ring A has a *natural inequality* with $a \neq b$ if and only if $a - b$ is invertible, with which A becomes a field by definition, and which is a ring inequality. The natural inequality is contained in (respectively, coincides with) an arbitrary inequality $\neq$ on A if and only if A is nontrivial (respectively, a field) with respect to $\neq$. In particular, the natural inequality is consistent (respectively, standard) if and only if A is nontrivial (respectively, a field classically) with respect to the denial inequality.

The natural inequality is cotransitive precisely when A is a *local ring*—that is,

$$a + b \in A^* \implies a \in A^* \vee b \in A^*$$

for all $a, b \in A$. An equivalent definition of a ring A to be local is that for each $a \in A$ either a is invertible or $1 - a$ is invertible. So a Heyting field is nothing but a local ring whose natural inequality is tight, with which it automatically is a nontrivial ring.

A subset S of A is a *coideal* [46] or *anti-ideal* [59, 8.3] whenever

$$\begin{array}{rcl} a \in S & \implies & \neg\,(a = 0) \\ a + b \in S & \implies & a \in S \vee b \in S \\ ab \in S & \implies & a \in S \wedge b \in S \end{array}$$

for all $a, b \in A$. By a *power coideal* we understand a coideal S of A with the additional property

$$a \in S \implies \forall n \in \mathbb{N}\ \left(a^n \in S\right)$$

for all $a \in A$. An arbitrary union of (power) coideals is a (power) coideal.

There is a characterisation of power coideals dual to that of radical ideals (Lemma 2).

---

21 If $\neq$ is translation invariant, then $\neq$ is cotransitive precisely when

$$a \neq b \implies a \neq c \vee c \neq b$$

for all $a, b, c \in A$, whose contrapositive amounts to $=$ being transitive whenever, in addition, $\neq$ is tight [6].

Lemma 3. *A subset S of a commutative ring A is a power coideal if and only if*

$$R(U) \between S \implies U \between S \tag{5}$$

for all (finite) $U \subset A$.

Proof. Suppose first that S is a power coideal, and let $a \in R(U)$, which is to say that $a^n \in I(U)$ for some $n \in \mathbb{N}$. If, in addition, $a \in S$, then also $a^n \in S$; in particular, $a^n \neq 0$. We thus have $a^n = r_1 b_1 + \cdots + r_m b_m$ for certain $m \in \mathbb{N}$, $r_1, \ldots, r_m \in A$, and $b_1, \ldots, b_m \in U$; whence $b_i \in S$ for some i, and b_i for this i is a witness for $U \between S$.

As for the converse, assume that (5) holds for all finite U. Note that $0 \notin S$ is the special case $U = \emptyset$ of (5), and let $a, b \in A$. If $ab \in S$, then $a \in S$ and $b \in S$ because $ab \in I(a) \cap I(b)$; if $a + b \in S$, then either $a \in S$ or $b \in S$ because $a + b \in I(a, b)$. Finally, if $a \in S$, then $a^n \in S$ because $a \in R(a^n)$. So S is a power coideal. □

A *prime coideal* of A is a coideal that, in addition, is a multiplicative subset of the ring A, where $S \subset A$ is a *multiplicative subset* if it is a submonoid of the multiplicative monoid of A, which is to say that

$$\begin{aligned} a \in S \wedge b \in S &\implies ab \in S \\ a = 1 &\implies a \in S \end{aligned}$$

for all $a, b \in A$. Among the detachable subsets of a ring with the denial inequality, the (respectively, power or prime) coideals are just the complements of the (respectively, radical or prime) ideals.

Clearly, the empty subset $\emptyset$ is a power coideal, but not a prime coideal. If S is a coideal, then S is inhabited precisely when $1 \in S$ or, equivalently, $A^* \subset S$. An inhabited coideal S of A is called a *minimal coideal* whenever for every $a \in S$ there is $b \in A$ so that $1 - ab \notin S$. If S is a minimal coideal and T an inhabited coideal with $T \subset S$, then $T = S$.

So every inhabited coideal lies between A^* and $\neg\{0\}$, and A is nontrivial whenever it has an inhabited coideal S with $S \subset \sim \{0\}$. The subset A^* is a coideal if and only if A is a local ring that is nontrivial with respect to the denial inequality, in which case A^* is even a minimal coideal. On the other hand, $\sim \{0\}$ is a coideal precisely when $\neq$ is cotransitive and—possibly except for being translation invariant—a ring inequality. If this is the case, then $\sim \{0\}$ is a power, prime, or minimal coideal if and only if A is a reduced ring, an integral domain, or a field, respectively.

The complement $\neg S$ of a (power) coideal S is a (radical) ideal, but the analogous statement for prime (co)ideals fails constructively: the set of invertible elements $\sim \{0\}$ in $\mathbb{R}$ or $\mathbb{C}$ is a minimal coideal, but $\{0\} = \neg \sim \{0\}$ is constructively not even a prime ideal in each of these Heyting fields (see above). So if $S \subset A$ is a coideal, then there is the factor ring $A/\neg S$, equipped with the ring apartness for which the equivalence classes $\neq 0$ are the ones of the elements of S.

Clearly, $A/\neg\emptyset$ is the trivial ring, and $A/\neg \sim \{0\}$ is isomorphic to A whenever A has come with a ring apartness. If S is a coideal, then S is inhabited precisely when $A/\neg S$ is nontrivial. Each coideal S is a power, prime, or minimal coideal if and only if $A/\neg S$ is a reduced ring, an integral domain, or a (Heyting) field, respectively. In particular, every minimal coideal is a prime coideal, and every prime coideal is a power coideal. If A^* is a coideal, then $A/\neg A^*$ is a Heyting field.

We often speak of prime coideals as of prime filters, following the use of this term in [28, p. 192]. To justify this, we recall that a subset S of a ring A is a *filter* whenever

$$\begin{array}{ccc} a = 1 & \Longrightarrow & a \in S, \\ a \in S \wedge b \in S & \Longrightarrow & ab \in S, \\ ab \in S & \Longrightarrow & a \in S \wedge b \in S \end{array}$$

for all $a, b \in A$, and a *prime filter* if, in addition,

$$\begin{array}{ccc} a + b \in S & \Longrightarrow & a \in S \vee b \in S, \\ a \in S & \Longrightarrow & \neg (a = 0) \end{array}$$

for all $a, b \in A$. Note that S is a prime filter if and only if it is a prime coideal if and only if it is a filter and a coideal. The smallest filter is A^*, which is a prime filter if and only if A is a local ring that is nontrivial with respect to the denial inequality (see above).

4. The covering relation

The basic ingredient of a formal topology is the underlying set A, which is often assumed to be a multiplicatively written commutative monoid with unit, and whose elements and subsets are called basic opens and arbitrary opens, respectively (Section 2). Furthermore, a definition of a formal topology must at least include a covering relation $\lhd$, between basic and arbitrary opens, with $a \lhd U$ being thought of as expressing that the basic open set with index $a \in A$ is contained in the union of all the basic open sets whose indices belong to $U \subset A$. In the following, we loosely follow Sambin's presentation of a formal topology [47,49].

For an arbitrary set A, the defining properties of a *covering relation* (or simply *covering*) $\lhd$ between elements and subsets of A are

$$\begin{array}{lccc} \textit{Reflexivity} & a \in U & \Longrightarrow & a \lhd U \\ \textit{Transitivity} & a \lhd U \wedge \forall b \in A\ (b \in U \Rightarrow b \lhd V) & \Longrightarrow & a \lhd V \end{array}$$

for all $a \in A$ and $U, V \subset A$. Equivalently, the operator $U \mapsto U^{\lhd}$ on the subsets of A with

$$U^{\lhd} = \{a \in A : a \lhd U\}$$

for $U \subset A$ is a *closure operator* on the subsets of A—that is, it satisfies

$$U \subset U^{\lhd}\ , \text{ and } U \subset V^{\lhd} \Longrightarrow U^{\lhd} \subset V^{\lhd}.$$

To extend $\lhd$ to a relation between arbitrary opens, one sets

$$U \lhd V \iff \forall b \in A\ (b \in U \Rightarrow b \lhd V)$$

for $U, V \subset A$; then transitivity can be rewritten more suggestively as

$$a \lhd U \wedge U \lhd V \Longrightarrow a \lhd V.$$

If A is a multiplicative monoid, then a covering relation $\lhd$ must also satisfy

$$\begin{array}{lccc} \textit{Left} & a \lhd U \vee b \lhd U & \Longrightarrow & ab \lhd U \\ \textit{Right} & a \lhd U \wedge a \lhd V & \Longrightarrow & a \lhd UV \end{array}$$

for all $a \in A$ and $U, V \subset A$, where

$$UV = \{bc : b \in U,\ c \in V\}$$

for $U, V \subset A$. (As usual, we denote the product $a \cdot b$ simply by ab.) Although one of the antecedents of 'left' could be left out in the commutative case, we prefer to follow [49] and write 'left' as it stands. 'Right', on the other hand, could equally be put with $a \lhd VU$ as the consequent, even if A is not commutative—which, however, we suppose from now on.

An equivalent of the conjunction of 'left' and 'right' is

$$U^{\lhd} \cap V^{\lhd} = (UV)^{\lhd}$$

for all $U, V \subset A$. This is equivalent to the set of conditions

Weakening	$ab \lhd a$
Contraction	$a \lhd aa$
Stability	$a \lhd U \wedge b \lhd V \implies ab \lhd UV$

for all $a \in A$ and $U, V \subset A$. (Here, as throughout, we identify each basic open a with the singleton arbitrary open $\{a\}$.) By reflexivity and transitivity of $\lhd$, moreover, stability amounts to

$$\textit{Localisation} \qquad a \lhd U \implies ab \lhd Ub$$

for all $a, b \in A$ and $U \subset A$. If, in addition, A possesses a unit 1, then reflexivity and 'left' yield that $a \lhd 1$ for all $a \in A$ or, equivalently, $1^{\lhd} = A$; whence $U \lhd 1$ for all $U \subset A$.

In a later version of formal topology [51,48], which was motivated by the need to dispense with the monoid structure, 'left' and 'right' have been generalised to

$$\textit{Down} \qquad a \lhd U \wedge a \lhd V \implies a \lhd U \downarrow V$$

with

$$U \downarrow V = \{d \in A : \exists b \in U\ (d \lhd b) \wedge \exists c \in V\ (d \lhd c)\}$$

for all $a \in A$ and $U, V \subset A$. Indeed, this does not involve the monoid multiplication, in whose presence 'down' follows from 'left' and 'right' by virtue of reflexivity and transitivity: then $UV \subset U \downarrow V \subset (UV)^{\lhd}$, so that $(U \downarrow V)^{\lhd} = (UV)^{\lhd}$. Note that the converse of 'down' is an immediate consequence of transitivity and reflexivity.

The *frame of arbitrary opens* $\mathrm{Open}\,(A)$ is the collection of subsets of A with zero $\emptyset$, unit A, meet $U \wedge V = UV$ (or, in the absence of a monoid operation, $U \wedge V = U \downarrow V$), join $\bigvee_{i \in I} U_i = \bigcup_{i \in I} U_i$, the partial order given by the covering $\lhd$, and the equality defined by setting

$$U \cong V \iff U \lhd V \wedge V \lhd U$$

for $U, V \subset A$. The closure operator $U \mapsto U^{\lhd}$ maps $\mathrm{Open}\,(A)$ isomorphically onto the *frame of formal opens* $\mathrm{Sat}\,(A)$, where an arbitrary open U is a *formal open* whenever it is *saturated* with respect to the covering relation—that is, U equals its *saturation* $U^{\lhd}$. The formal opens form a frame $\mathrm{Sat}\,(A)$ with zero $\emptyset^{\lhd}$, unit A, meet $U \wedge V = U \cap V$ (which equals $(UV)^{\lhd}$ and, more generally, $(U \downarrow V)^{\lhd}$), join $\bigvee_{i \in I} U_i = \left(\bigcup_{i \in I} U_i\right)^{\lhd}$, the partial order given by inclusion, and the extensional equality of subsets as equality.

It depends on the given context whether one decides to work with Open (A) or Sat (A). Note that the covering relation suffices to define both frames; there is no need of a monoid structure. As either frame is a relatively unrestricted collection of subsets of the given set A, both Open (A) and Sat (A) must be secondary to formal topology as a predicative framework.

Of course, one could represent any given frame as the frame of (formal) opens of a formal topology, with the names of a basis of that frame as the underlying set—provided, however, that one can choose those names in such a way that they indeed form a set, which is not clear at the outset. In this vein, formal topology can be understood as predicative presentation of frames.

A covering $\lhd$ is a *Stone covering* or *finitary covering* if every basic open a is compact in the sense that if $a \lhd U$ for an arbitrary open U, then already $a \lhd U_0$ for some finite subset U_0 of U. If the underlying set is a multiplicative monoid, and if $\lhd$ satisfies 'left' and 'right',[22] then $\lhd$ is finitary precisely when the corresponding frame of (formal) opens is a coherent frame—or, equivalently, a spectral locale. A formal topology with a covering of this kind is simply called a *Stone formal topology* or *finitary formal topology*.

The *Stone compactification* $\preceq$ of a relation $\prec$, between basic opens and finite arbitrary opens, is defined by setting $a \preceq U$ precisely when $a \prec U_0$ for some finite $U_0 \subset U$. If $\lhd$ is a Stone covering, then it coincides with the Stone compactification of its *finitary trace* which is the induced relation between basic opens and finite arbitrary opens. We refer to [47,40,41] for details on all this.

Now let A be a commutative ring. According to what we have observed before, we take the multiplicative monoid of A as underlying to the formal Zariski topology associated with A. The clue to a covering relation on this monoid is to remember that, within the classical Zariski topology on Spec(A),

$$D(a) \subset \bigcup_{b \in U} D(b) \iff a \in R(U)$$

for all $a \in A$ and $U \subset A$; see [28, V.3.2] for the analogous observation in the case of the reticulation of A.

In view of the aforementioned intuition standing behind $a \lhd U$, it is appropriate to follow Persson [44] by setting

$$a \lhd U \iff a \in R(U)$$

for all $a \in A$ and $U \subset A$. Note that $I(\emptyset) = 0$, so that

$$R(\emptyset) = \left\{a \in A : \exists n \in \mathbb{N}\ \left(a^n = 0\right)\right\}$$

is the nilradical of A. In particular,

$$a \lhd \emptyset \iff \exists n \in \mathbb{N}\ \left(a^n = 0\right)$$

for every $a \in A$.

[22] We are grateful to Silvia Gebellato for having pointed out to us these necessary preconditions.

We carry out the next proof in detail, although most of it is in [44].

Proposition 4. *Let A be a commutative ring. Then $\lhd$ is a covering relation: that is, it is reflexive and transitive, and satisfies 'left' and 'right'. In other words, R is a closure operator with $U^{\lhd} \cap V^{\lhd} = (UV)^{\lhd}$ for all $U, V \subset A$.*

Proof. Let $a \in A$ and $U, V \subset A$. As $R(U)$ is a radical ideal containing U, we have 'left', reflexivity, and transitivity (Lemma 2). Suppose now that $a \lhd U$ and $a \lhd V$, that is, $a^p \in I(U)$ for some $p \in \mathbb{N}$ and $a^q \in I(V)$ for some $q \in \mathbb{N}$. Then $a^{p+q} \in I(U) I(V) \subset I(UV)$, so that $a \lhd UV$, and 'right' is proved. $\square$

It is intrinsic to the very definition of $\lhd$ that it is a Stone covering; we have already made use of this fact in the foregoing proof. As R is the corresponding closure operator, the frame of formal opens is the Zariski frame of A.

We now relate $\lhd$ to the covering defined by Lombardi and Quitté [32]. They say, for multiplicative submonoids $S, S_1, \ldots, S_m$ of A, that S is covered by $S_1, \ldots, S_m$ whenever $S \between I(s_1, \ldots, s_m)$ for all $s_1 \in S_1, \ldots, s_n \in S_m$. In this vein, we set $a \sqsubset \{b_1, \ldots, b_m\}$ for $a \in A$ and $b_1, \ldots, b_m \in A$ precisely when the multiplicative submonoid $M(a)$ generated by a is covered by $M(b_1), \ldots, M(b_m)$. This relation $\sqsubset$ coincides with the finitary trace of $\lhd$; in particular, $\lhd$ coincides with the Stone compactification of $\sqsubset$.

In fact, $a \sqsubset \{b_1, \ldots, b_m\}$ if and only if $M(a) \between I(b_1^{k_1}, \ldots, b_m^{k_m})$ for all $k_1, \ldots, k_m \geq 0$; which clearly implies $a \lhd \{b_1, \ldots, b_m\}$ (just set $k_i = 1$ for every i). To see the converse, assume that $a \lhd \{b_1, \ldots, b_m\}$, which is to say that $a^p \in I(b_1, \ldots, b_m)$ for some $p \in \mathbb{N}$. Given $k_1, \ldots, k_m \geq 0$, set $k = \max\{k_1, \ldots, k_m\}$. Then $a^{pmk} \in I(b_1^k, \ldots, b_m^k) \subset I(b_1^{k_1}, \ldots, b_m^{k_m})$ by Lemma 1; whence $a \sqsubset \{b_1, \ldots, b_m\}$.

It is in order to end this section by considering a possible objection. A covering relation is in general an *infinitary* relation: it relates elements of A with possibly *infinite* subsets of A. This may cause doubts from a strictly predicative perspective from which one prefers not to consider infinite subsets at all; more specifically, one can well argue that already the definition of a relation to be a covering consists in a universal quantification not only over the basic opens, but also over the arbitrary opens. (The same concerns will come up when we next deal with the positivity relation.)

In the context of the formal Zariski topology, however, there is absolutely no need to worry about this: as for every *finitary* covering, it indeed suffices to restrict one's attention to *finite* subsets of A. In general, moreover, one ought to observe that the defining properties of a covering are only to be satisfied by a relation that is already given, or presented by other means, whereas these properties do not enter its very construction—unless one wishes to define it as the narrowest relation possessing those properties, but even such inductive definitions allow for a predicatively admissible modification. We refer to Section 6.1 and to the discussion preceding it for more on this.

5. A candidate for positivity

In addition to a covering relation, one wishes to have at hand whenever possible a notion of a 'positivity' whose unary version, a predicate $\mathrm{pos}(a)$ of basic opens $a \in A$, expresses the intuition that the basic open set with index a is inhabited. One of the roots of this so-called positivity predicate is the consistency predicate from domain theory [53,48,41]; another one is the impredicative notion of positivity in locale theory (see below). We shall elaborate in Section 6 on the more general notion of a positivity relation.

We first recall the concept of a positivity predicate from [47]. Given a set A with a covering relation $\lhd$ as above, a *positivity predicate* or *unary positivity* is a predicate $\mathrm{pos}(a)$ of elements a of A. It is usually expected to satisfy

$$\begin{array}{lccc} \textit{Monotonicity} & \mathrm{pos}(a) \wedge a \lhd U & \Longrightarrow & \mathrm{pos}(U) \\ \textit{Openness} & a \lhd U & \Longrightarrow & a \lhd U^{+} \end{array}$$

with the notation

$$\begin{array}{ccc} \mathrm{pos}(U) & \Longleftrightarrow & \exists b \in U \ \ (\mathrm{pos}(b)) \\ U^{+} & = & \{b \in U : \mathrm{pos}(b)\} \end{array}$$

for all $a \in A$ and $U \subset A$.

However, as the instances of such a predicate that we will encounter in the sequel are almost never both monotone and open, we shall use the terms ‘positivity predicate’ and ‘unary positivity’ for each predicate—neither necessarily monotone nor open—that we consider as a candidate for such a notion, and make explicit when it enjoys one of these properties.

In the presence of openness, monotonicity is tantamount to

$$\textit{Weak Monotonicity} \qquad \mathrm{pos}(a) \wedge a \lhd U \implies \exists b \in U.$$

Weak monotonicity and openness ensure that *if* there is a predicate satisfying both conditions, *then* it is unique. More specifically, if pos_1 is a weakly monotone predicate and pos_2 is open, then pos_1 is contained in pos_2. (We have first seen all this in [18].)

In Section 4, we have satisfactorily dealt with the covering relation for the formal Zariski topology of a commutative ring A. We now turn our attention to the question how to complete this picture with a positivity predicate.

Classically, the nilradical of A is the intersection of all prime ideals, in other words

$$\exists n \in \mathbb{N} \left(a^n = 0\right) \iff \forall \mathfrak{p} \in \mathrm{Spec}(A)\,(a \in \mathfrak{p}),$$

so that, still classically,

$$\forall n \in \mathbb{N} \left(a^n \neq 0\right) \iff \exists\, \mathfrak{p} \in D(a)$$

for all $a \in A$. Hence it is tempting to consider the left-hand side of the latter equivalence as a possible candidate for a unary positivity.

In this vein, we set

$$\mathrm{Pos}_0(a) \iff \forall n \in \mathbb{N} \left(a^n \neq 0\right)$$

for every $a \in A$. Note that if $\neq$ is a ring inequality, then $\mathrm{Pos}_0(a)$ amounts to the existence of infinitely many n with $a^n \neq 0$ (if $a^m \neq 0$, then $a^n \neq 0$ for all $n \leq m$ because $a^m = a^n a^{m-n}$).

Clearly, Pos_0 is weakly monotone: for $a \in A$ and $U \subset A$, if $\mathrm{Pos}_0(a)$ and $a \lhd U$, then $a^n \in I(U)$ for some n and $a^n \neq 0$ also for this n, so that U is inhabited.

As a by-product of the subsequent considerations, we shall see that Pos_0 is open precisely when A has recognisable nilpotents, in which case it is a decidable predicate, and that Pos_0 is monotone under slightly more general circumstances.

5.1. Monotonicity

We now investigate whether and when Pos_0 is monotone.

Lemma 5. *Let* pos *be a predicate on a commutative ring A. Then $\{a \in A : \mathrm{pos}(a)\}$ is a power coideal if and only if* pos *is monotone.*

Proof. This is nothing but a reformulation of Lemma 3; in particular, if pos satisfies monotonicity for $U = \emptyset$, then $\mathrm{pos}(a)$ implies $\neg(a = 0)$ for all $a \in A$. □

This helps us to characterise the monotonicity of Pos_0.

Lemma 6. *Let A be a commutative ring with a ring inequality $\neq$.*

1. *If $\neq$ is cotransitive, then*
$$\forall n \in \mathbb{N}\ \big((a+b)^n \neq 0\big) \implies \forall n \in \mathbb{N}\ \big(a^n \neq 0 \vee b^n \neq 0\big)$$
for all $a, b \in A$.
2. Pos_0 *is monotone if and only if*
$$\mathrm{Pos}_0(a+b) \implies \mathrm{Pos}_0(a) \vee \mathrm{Pos}_0(b) \tag{6}$$
for all $a, b \in A$.

Proof. We first prove the first statement. For arbitrary $n \in \mathbb{N}$, if $(a+b)^{2n} \neq 0$, then $a^n \neq 0$ or $b^n \neq 0$ whenever $\neq$ is cotransitive: recall that $(a+b)^{2n} \in I(a^n, b^n)$ as in Lemma 1. As $\{a \in A : \mathrm{Pos}_0(a)\}$ has a priori all the defining properties a power coideal except for (6), the second statement follows from Lemma 5. □

As any infinite conjunction, $\mathrm{Pos}_0(a)$ is hard to verify unless it actually is a finite one. When looking for neat conditions under which this is the case, one might tentatively assume that the commutative ring A under consideration is reduced. Indeed, Pos_0 is monotone whenever A is a reduced ring and $\neq$ a cotransitive ring inequality.

Many rings one might at first think of are reduced whenever they are equipped with their usual inequalities. However, it is not recommended at all to restrict one's attention to reduced rings from the outset, because it is just the admission of non-zero nilpotents—which, as algebraic infinitesimals, are indispensable for deformation theory—that to a large extent makes up the power of modern algebraic geometry. (Compared with reducedness, it is fairly mild to assume that the rings under consideration have a cotransitive ring inequality.)

As soon as one has a closer—classical—look at the variety of rings naturally arising in algebraic geometry, one realises that $\mathrm{Pos}_0(a)$ is still a finite conjunction for most such rings A and every $a \in A$.[23] More specifically, and classically speaking, every finitely generated

23 The author is indebted to Otto Forster for having hinted at this circumstance.

algebra A over a Noetherian ring is also Noetherian (by Hilbert's basis theorem); whence the nilradical of any such A possesses a finite set of generators.[24] Therefore the nilradical of A is nilpotent: that is, one can find $k \in \mathbb{N}$ such that

$$\exists n \in \mathbb{N} \left(a^n = 0\right) \implies a^k = 0$$

for all $a \in A$.

In this vein, we call a ring A *quasireduced* if for every $a \in A$ there is $k \in \mathbb{N}$ with

$$a^k \neq 0 \implies \forall n \in \mathbb{N}\,(a^n \neq 0),$$

and say that the ring A is *uniformly quasireduced* if such a k can be chosen independently of a: as a *universal exponent* for A.[25] If $\neq$ is a ring inequality, then the principal issue of (uniform) quasireducedness is that $a^n \neq 0$ for all the $n > k$ (because $a^k \neq 0$ automatically implies that $a^n \neq 0$ for all $n \leq k$). Needless to say, every reduced ring is uniformly quasireduced, with universal exponent 1.

Every ring with recognisable nilpotents is quasireduced, and uniformly quasireduced provided that, in addition, its nilradical is nilpotent. Indeed, if $a^n \neq 0$ for all n, then there is nothing to prove, whereas if $a^k = 0$ for some $k \in \mathbb{N}$, then $a^k \neq 0$ is impossible, and any such k is a universal exponent whenever it may be chosen independently of the nilpotent a under consideration. Conversely, every discrete (uniformly) quasireduced ring has recognisable nilpotents (and a nilpotent nilradical): given k as in the definition of '(uniformly) quasireduced', we can decide whether $a^k = 0$ or $a^k \neq 0$.

So quasireducedness is a classically trivial property, which its uniform version is not. The standard example

$$B = \mathbb{Z}[T_1, T_2, T_3, \ldots] \Big/ I \left(T_1^2, T_2^3, T_3^4, \ldots\right)$$

of a ring whose nilradical is not nilpotent, let alone finitely generated, serves well as an example of a ring that is not even classically uniformly quasireduced.[26] We understand B to be equipped with the usual equality of equivalence and the corresponding denial inequality, with which it clearly is discrete, and we write t_n for the equivalence class of each T_n.

If B were uniformly quasireduced with a universal exponent k, then $t_k^n \neq 0$ for all n (because clearly $t_k^k \neq 0$), which would contradict the fact that $t_k^n = 0$ for every $n \geq k + 1$.

---

24 This classical understanding of 'Noetherian', that every ideal is finitely generated, is constructively void already for the ideals of the field with two elements. We refer to [38, III.2, VIII.1] for constructively meaningful variants of 'Noetherian' and Hilbert's basis theorem.

25 Equivalently, A is quasireduced whenever

$$\forall a \in A\, \exists k \in \mathbb{N}\, \forall n \in \mathbb{N} \left(a^k \neq 0 \Longrightarrow a^n \neq 0\right),$$

and uniformly quasireduced whenever

$$\exists k \in \mathbb{N}\, \forall a \in A\, \forall n \in \mathbb{N} \left(a^k \neq 0 \Longrightarrow a^n \neq 0\right).$$

Silvia Gebellato has kindly drawn our attention to these formulations.

26 The author is grateful to Helmut Zöschinger for reminding him of this example.

On the other hand, B has recognisable nilpotents, since for every $F \in \mathbb{Z}[T_1, T_2, T_3, \ldots]$ the equivalence class $f \in B$ of F is (not) nilpotent whenever the constant term $F(0)$ of F is (not) equal to 0, which is a decidable alternative. Indeed, there is $k \in \mathbb{N}$ with $F \in \mathbb{Z}[T_1, \ldots, T_k]$, so that if $F \in I(T_1, \ldots, T_k)$ is a sum of m nonconstant monomials, then $F^{m(k+1)} \in I(T_1^{k+1}, \ldots, T_k^{k+1})$ according to Lemma 1, and thus $f^{m(k+1)} = 0$.

The advantage of working in a quasireduced ring A is that to verify a finite—actually, a singleton—conjunction suffices to achieve the validity of the infinite conjunction $\mathrm{Pos}_0(a)$.

Proposition 7. *Let A be a commutative ring. If A is quasireduced and comes with a cotransitive ring inequality $\neq$, then* Pos_0 *is monotone.*

Proof. We make use of both parts of Lemma 6. Let $a, b \in A$. As A is quasireduced, there are $p, q \in \mathbb{N}$ so that if $a^p \neq 0$, then $\mathrm{Pos}_0(a)$, and if $b^q \neq 0$, then $\mathrm{Pos}_0(b)$. Set $k = \max\{p, q\}$. If $\mathrm{Pos}_0(a + b)$, then either $a^k \neq 0$ and thus $a^p \neq 0$, or $b^k \neq 0$ and thus $b^q \neq 0$. $\square$

To present an interesting class of rings that are constructively uniformly quasireduced, we consider, for arbitrary $k \in \mathbb{N}$, the ring

$$C_k = C[T]/I(T^k)$$

whose prime spectrum is the k-fold point over a Heyting field C. More precisely, $C_k = C[T]/\neg \sim I(T^k)$ with $\neg \sim I(T^k) = I(T^k)$ according to [59, 8.5]. We write t for the equivalence class of T; whence $t^k = 0$ and $C_k = C[t]$, and equality and inequality are so that

$$\sum_{i=0}^{k-1} \nu_i t^i = 0 \iff \forall i < k\, (\nu_i = 0),$$
$$\sum_{i=0}^{k-1} \nu_i t^i \neq 0 \iff \exists i < k\, (\nu_i \neq 0).$$

Now let $c = \sum_{i=0}^{k-1} \nu_i t^i \in C_k$, fix $n \in \mathbb{N}$ for the moment, and write $c^n = \sum_{i=0}^{k-1} \mu_i^{(n)} t^i$. Then $\mu_0^{(n)} = \nu_0^n$, and $\mu_i^{(n)}$ is a multiple of ν_0 whenever $i < \min\{n, k\}$. It is routine to verify that

$$\exists n \in \mathbb{N}\ (c^n = 0) \iff \nu_0 = 0 \iff c^k = 0$$
$$\forall n \in \mathbb{N}\ (c^n \neq 0) \iff \nu_0 \neq 0 \iff c^k \neq 0$$

for all $c \in C_k$. So C_k, which is reduced only for $k = 1$, is uniformly quasireduced for every $k \in \mathbb{N}$, with this k as a universal exponent. Note that C_k has recognisable nilpotents (equivalently, C_k is discrete) precisely when C is discrete.

However, general discrete rings are constructively far from being quasireduced.

Proposition 8. *The following items are equivalent.*

1. *The limited principle of omniscience (LPO).*
2. *Every discrete commutative ring has recognisable nilpotents.*
3. *Every discrete commutative ring is quasireduced.*

Proof. It remains to show that the last item implies the first. To this end, let $(\lambda_n)_{n\in\mathbb{N}}$ be an increasing sequence in $\{0, 1\}$, and equip

$$D = \mathbb{Z}[T]/I(\{\lambda_n T^n : n \in \mathbb{N}\})$$

with the equality of equivalence and the corresponding denial inequality. We write t for the equivalence class of T; whence $D = \mathbb{Z}[t]$ with

$$t^n = 0 \iff \lambda_n = 1 \quad \text{and} \quad t^n \neq 0 \iff \lambda_n = 0\,.$$

Then it is easy to show that D is discrete. If D is quasireduced, then there is $k \in \mathbb{N}$ so that if $t^k \neq 0$, then $t^n \neq 0$ for all n. Now we either have $t^k = 0$ or $t^k \neq 0$. In the former case, $\lambda_k = 1$ for this k, whereas in the latter case $\lambda_n = 0$ for all n. □

Note that LPO already follows from the second or third item of Proposition 8 when this is restricted to discrete commutative rings that, as $\mathbb{Z}$-algebras, have a single generator—as the ring D in the proof.

The converse of Proposition 7 cannot be expected to hold constructively in general.

Corollary 9. *LPO follows from the statement that, for every discrete commutative ring A, if* Pos_0 *is monotone, then A is quasireduced.*

Proof. It suffices to verify, by the second part of Lemma 6, that Pos_0 is monotone for the ring D in the proof of Proposition 8. To this end, let $f, g \in D$. If $f(0) \neq 0$, then $f^n = f(0)^n + t(\ldots) \neq 0$ for all n, and likewise if $g(0) \neq 0$, so that there is nothing to prove. Hence we may assume that $f(0) = g(0) = 0$, in which case $f + g$ is a multiple of t^ℓ for some $\ell \in \mathbb{N}$. If now $\mathrm{Pos}_0(f+g)$, then $t^{\ell n} \neq 0$ for all n; whence $\lambda_n = 0$ for all n and thus $D = \mathbb{Z}[T]$ is reduced, so that $\mathrm{Pos}_0(f)$ or $\mathrm{Pos}_0(g)$ as required. □

One cannot even prove constructively that Pos_0 is monotone for an arbitrary discrete ring.[27]

Proposition 10. *The following items are equivalent.*

1. *The lesser limited principle of omniscience (LLPO).*
2. *For every discrete commutative ring A and all $a, b \in A$,*

$$\forall n \in \mathbb{N}\, \left(a^n \neq 0 \vee b^n \neq 0\right) \implies \forall n \in \mathbb{N}\, \left(a^n \neq 0\right) \vee \forall n \in \mathbb{N}\, \left(b^n \neq 0\right)\,.$$

3. Pos_0 *is monotone for every discrete commutative ring.*

Proof. To deduce the second item from LLPO, let A be a discrete commutative ring, and $a_0, a_1 \in A$ such that for each $n \in \mathbb{N}$ either $a_0^n \neq 0$ or $a_1^n \neq 0$. Now define iteratively a sequence $(\lambda_n)_{n\in\mathbb{N}}$ in $\{0, 1\}$ by setting $\lambda_1 = 0$ and

$$\begin{aligned}
\lambda_{2k+i} = 0 &\iff a_i^k \neq 0 \vee \exists m < 2k + i\ (\lambda_m = 1)\\
\lambda_{2k+i} = 1 &\iff a_i^k = 0 \wedge \forall m < 2k + i\ (\lambda_m = 0)
\end{aligned}$$

[27] The author thanks Douglas Bridges for encouraging him to keep to LLPO in this context.

for each $i \in \{0, 1\}$ and every $k \in \mathbb{N}$, for which clearly $\lambda_n = 1$ for at most one n. If we assume that LLPO is valid, then $\lambda_{2k+i} = 0$ for some $i \in \{0, 1\}$ and all $k \in \mathbb{N}$. Hence $a_i^n \neq 0$ for this i and all n. Indeed, if for any k there is $m < 2k + i$ with $\lambda_m = 1$, then $m = 2\ell + 1 - i$ for some ℓ. Therefore $a_{1-i}^{\ell} = 0$ and thus $a_{1-i}^n = 0$ for all $n \geq \ell$, so that $a_i^n \neq 0$ for all n.

To show that the second item implies the third, it suffices to invoke both parts of Lemma 6. To regain LLPO from the last item, let $(\lambda_n)_{n\in\mathbb{N}}$ be a sequence in $\{0, 1\}$ with $\lambda_1 = 0$ and $\lambda_n = 1$ for at most one n, and set

$$E = \mathbb{Z}[T_0, T_1]/I(\{T_i^k : \lambda_{2k+i} = 1,\ k \in \mathbb{N},\ i \in \{0, 1\}\}) .$$

Equipped with the equality of equivalence and the corresponding denial inequality, E is discrete. Indeed, if we write t_i for the equivalence class of T_i, then

$$\begin{aligned} t_i^n = 0 &\iff \exists k \leq n\ (\lambda_{2k+i} = 1) \\ t_i^n \neq 0 &\iff \forall k \leq n\ (\lambda_{2k+i} = 0) \end{aligned}$$

for each $i \in \{0, 1\}$ and $n \in \mathbb{N}$. It is routine to verify that $\mathrm{Pos}_0\,(t_0 + t_1)$, so if Pos_0 is monotone for E, then, by the second part of Lemma 6, $\mathrm{Pos}_0\,(t_i)$ for some $i \in \{0, 1\}$; whence $\lambda_{2k+i} = 0$ for this i and all $k \in \mathbb{N}$. $\square$

As with Proposition 8, to achieve LLPO it suffices to assume the second or third item of Proposition 10 for every discrete commutative ring that, as a $\mathbb{Z}$-algebra, has two generators, such as the ring E in the proof.

In particular, weak monotonicity is (constructively) weaker than monotonicity.

5.2. Openness

Apart from the trivial case of a ring with recognisable nilpotents, the openness of Pos_0 will turn out to be essentially nonconstructive even in situations in which Pos_0 is monotone. We now attempt to justify this seeming defect, which eventually will prove to be unavoidable even in the case of a fairly simple discrete ring.

First, the presence of an open and monotone positivity predicate on a formal topology is equivalent to the corresponding frame of opens being an open locale as defined, for instance, in [29] (see [18] for more details). An arbitrary locale L is open if and only if for each $\mathcal{U} \subset L$ covering some $U \in L$ the subset $\mathcal{U}^+$ of $\mathcal{U}$ consisting of its positive elements still covers U; in other words, the nonpositive elements are irrelevant for the covering, and thus may be left out. But what does 'positive' mean?

The locale-theoretic definition of an element U of L to be positive is that every subset $\mathcal{U}$ of L which covers U is inhabited. As this involves quantification over the subsets of L, it is an impredicative definition. Therefore it had to be given up in formal topology, where instead a positivity predicate was stipulated as an extra datum. Monotonicity was introduced as an axiom to capture the meaning of 'positive', and openness as a useful condition that later turned out to correspond to the concept of an open locale.

From this perspective, openness is more loosely tied to the notion of a positivity predicate than monotonicity is: as for locales, openness is an extra feature that may be given in some but not all cases. Note also that openness has a certain flavour of point-set topology: every spatial locale is open [29, p. 99], and if a formal topology has enough (formal) points, then openness holds (Proposition 26 below).

In [15, Proposition 5], monotonicity and openness were justified by the observation that *if* a formal topology carries a monotone and open pos, *then* pos (a) is equivalent to POS (a) for every basic open a, where the latter is defined—as impredicatively as 'positive' in locale theory—by setting

$$\mathrm{POS}\,(a) \iff \forall U \subset A\ (a \lhd U \Rightarrow \exists b \in U)$$

for every a. More specifically, if pos is weakly monotone, then pos (a) implies $\mathrm{POS}(a)$ for every basic open a, and if pos is open, then the reverse implication holds. Note that POS is weakly monotone by its very definition.

In other words, while the weak monotonicity of a predicatively presented pos guarantees that it stays within its impredicative counterpart POS, openness ensures that the former fully covers the meaning of the latter. Just as when passing to constructive reasoning, however, one often needs to strengthen some concepts when one wishes to admit predicative definitions only. It therefore is not surprising to encounter positivity predicates that are (weakly) monotone, but fail to be open constructively.

Next, openness allows us to drop the nonpositive elements of an arbitrary open that covers a basic open without deciding the possibly nonconstructive alternative whether any given element of the former is positive or not. In proof practice, openness even allows us to certain distinctions-by-cases that otherwise would have to be left out for then remaining purely classical.

To explain this in more details, let A for the moment denote an arbitrary set with a (reflexive and transitive) covering relation $\lhd$. According to [47,53], openness is equivalent, within intuitionistic logic, to the conjunction of the two conditions

$$\begin{array}{lccl} \textit{Proofs by cases} & (\mathrm{pos}(a) \Rightarrow a \lhd U) \wedge (\neg\mathrm{pos}(a) \Rightarrow a \lhd U) & \Longrightarrow & a \lhd U \\ \textit{Ex falso quodlibet} & \neg\mathrm{pos}(a) & \Longrightarrow & a \lhd \emptyset \end{array}$$

for all $a \in A$ and $U \subset A$.

The converse of '*ex falso quodlibet*', and that $\mathrm{pos}(a)$ implies $\neg\,(a \lhd \emptyset)$, are immediate consequences of weak monotonicity. If pos is a decidable predicate, then 'proofs by cases' trivially holds; whence openness is equivalent to '*ex falso quodlibet*' in any such case.

The following observation is readily made.

Lemma 11. *Let* pos *be a weakly monotone predicate on a set A with a covering relation $\lhd$. Then* pos *is decidable and satisfies* 'ex falso quodlibet' *precisely when for every $a \in A$ either* $\mathrm{pos}(a)$ *or $a \lhd \emptyset$. In this case,* pos *is open, and* $\mathrm{pos}(a)$ *and $a \lhd \emptyset$ are the negations of each other.*

As $\lhd$ is reflexive and transitive, one may replace the only occurrence of $\emptyset$ in '*ex falso quodlibet*' by that of an arbitrary $U \subset A$. Besides perhaps justifying the choice of the name for '*ex falso quodlibet*', this observation makes visible that

$$\textit{Positivity}\quad (\mathrm{pos}(a) \Rightarrow a \lhd U) \implies a \lhd U$$

for all $a \in A$ and $U \subset A$ is another equivalent of openness [47].

When one proves directly that positivity is equivalent to openness, one realises the analogous fact that ‘proofs by cases’ is tantamount to

$$a \lhd U \implies a \lhd U^+ \cup U^- \tag{7}$$

for all $a \in A$ and $U \subset A$, where

$$U^- = \{b \in U : \neg\mathrm{pos}(b)\}\,.$$

The following result sharpens a proposition by Negri [41].

Proposition 12. *Let* pos *be a weakly monotone predicate on a set* A *with a Stone covering* $\lhd$. *Then* pos *is decidable if and only if it satisfies ‘proofs by cases’.*

Proof. The ‘only if’ part is obvious. As for the ‘if’ part, let $a \in A$, and assume that (7) holds for $U = \{a\}$. As $a \lhd a$, we thus have $a \lhd a^+ \cup a^-$. Since $\lhd$ is a Stone covering, there is a finite subset U_0 of $a^+ \cup a^-$ with $a \lhd U_0$. As a finite set, U_0 is either empty or inhabited. In the former case, $a \lhd \emptyset$ and thus $\neg\mathrm{pos}(a)$, because pos is weakly monotone. In the latter case, there is $b \in U_0$, for which either $b \in a^+$ or $b \in a^-$. If $b \in a^+$, then b equals a and $\mathrm{pos}(b)$, so that $\mathrm{pos}\,(a)$. If $b \in a^-$, then b equals a and $\neg\mathrm{pos}(b)$, so that $\neg\mathrm{pos}\,(a)$. □

By virtue of Lemma 11, we have an obvious consequence.

Corollary 13. *Let* pos *be a weakly monotone predicate on a set* A *with a Stone covering* $\lhd$. *Then* pos *is open if and only if for every* $a \in A$ *either* $\mathrm{pos}(a)$ *or* $a \lhd \emptyset$.

Let now again A be a commutative ring. In general, $\mathrm{Pos}_0\,(a)$ is equivalent to $\neg\,(a \lhd \emptyset)$ whenever $\neq$ is the denial inequality. By Corollary 13, Pos_0 is open precisely when A has recognisable nilpotents. ‘*Ex falso quodlibet*’ and ‘proofs by cases’ for Pos_0 are equivalent to A having semirecognisable nilpotents and weakly recognisable nilpotents, respectively (for the latter, see Proposition 12).

However, we cannot expect a constructive proof, valid for arbitrary discrete A, that Pos_0 satisfies any of those equivalents. This is made explicit by the following three propositions, for which we refer to Proposition 8 and to Corollary 13 (and, wherever necessary, to the proof of the former). One might also compare them with the facts that LPO is equivalent to the conjunction of WLPO and MP, and that ‘open’ amounts to ‘proofs by cases’ and ‘*ex falso quodlibet*’.

Proposition 14. *The following items are equivalent.*

1. *The limited principle of omniscience (LPO).*
2. *For every discrete commutative ring* A *and every* $a \in A$ *either* $\mathrm{Pos}_0(a)$ *or* $a \lhd \emptyset$.
3. Pos_0 *is open for every discrete commutative ring.*

Proposition 15. *The following items are equivalent.*

1. *The weak limited principle of omniscience (WLPO).*
2. *Every discrete commutative ring has weakly recognisable nilpotents.*
3. Pos_0 *satisfies ‘proofs by cases’ for every discrete commutative ring.*

Proposition 16. *The following items are equivalent.*

1. *Markov's principle (MP).*
2. *Every discrete commutative ring has semirecognisable nilpotents.*
3. Pos_0 *satisfies* 'ex falso quodlibet' *for every discrete commutative ring.*

As with Proposition 8, to deduce the first item in each of the foregoing propositions from the second or third it suffices to suppose the latter for discrete commutative rings that, as $\mathbb{Z}$-algebras, have a single generator.

For a general commutative ring A, if Pos_0 is open, then Pos_0 is decidable and A is quasireduced (because A has recognisable nilpotents in any such case, see Corollary 13); whence Pos_0 is monotone provided that, in addition, A comes with a cotransitive ring inequality (Proposition 7). However, we cannot expect a constructive proof of the reverse implication for arbitrary discrete A.

Corollary 17. *LPO follows from the statement that, for every discrete commutative ring* A*, if* Pos_0 *is monotone, then it is open.*

Proof. Let $A = D$ be the discrete ring given in the proof of Proposition 8. Then Pos_0 is monotone for this ring (see the proof of Corollary 9). If Pos_0 is open, then Proposition 14 applies. $\square$

A related result in a (yet) different context is [15, Corollary 3].[28] As a consequence of Corollary 17, notice that if every positivity predicate pos on a Stone formal topology is open whenever it is monotone, then LPO holds. In particular, openness is constructively independent of monotonicity for Stone formal topologies.[29]

In the most general version of a basic formal topology to be recalled in the next section—when a positivity predicate is derived from a positivity relation—it does not make much sense to ask for openness (Corollary 25), whereas one always has monotonicity for granted. Moreover, one gets back nothing but Pos_0 whenever this is monotone (Proposition 22), a condition which is classically trivial but essentially nonconstructive (Corollary 24). Therefore we do not regret that Pos_0 fails in general to be open and monotone constructively, although it was designed to meet the intended meaning of a positivity predicate as perfectly as possible.

6. The positivity relation

We now extend the formal Zariski spectrum by defining a binary positivity, or positivity relation, along the lines of the so-called basic picture. Roughly speaking, the *basic*

---

28 Thierry Coquand has kindly pointed out this reference to us, where—although this was not made explicit—the nonconstructive character of a certain inductive positivity predicate is equally caused by its openness only.

29 This contrasts to the context of locales, at least in the presence of a certain version of the axiom of choice: that of the prime ideal theorem for distributive lattices [28, p. 78]. Then every spectral locale is spatial [28, II.3.4], and thus open [29, p. 99]. That every spectral locale is open hinges upon the presence of the axiom of choice: in topos theory there is a simple example, based on the Sierpinski locale, of a spectral locale that is not open. We owe the latter information to Steve Vickers, who ascribes it to Peter Johnstone.

picture has been started in a series of papers by Gebellato and Sambin [51,50,22,23] as a systematic method of studying the interplay between the so-called concrete aspects of topological spaces and continuous mappings that involve points, and their formal, point-free counterparts. So far a wealth of connections (symmetries, isomorphies, and dualities) has been revealed by way of the basic picture, of which we shall soon employ a fairly fundamental one for heuristic purposes.

Before so doing, it is in order to sketch an elementary but principal motivation for adding the notion of a binary positivity to the data of a formal topology. To this end, let A be a basis of open sets of a topological space X (in the concrete sense, based on points), and consider A as the underlying set of the corresponding formal topology. For the sake of the argument, we do not bother about issues of predicativity during this heuristic consideration, so whether any such A really is a set.

For $x, y \in X$, $T \subset X$, $a, b \in A$, and $U \subset A$, the naturally given covering $\lhd$ on A is so that membership of the formal closure

$$a \in U^{\lhd} \iff \forall y \in a \;\; \exists b \ni y \;\; (b \in U) \tag{8}$$

is completely symmetric to membership of the concrete closure

$$x \in \overline{T} \iff \forall b \ni x \;\; \exists y \in b \;\; (y \in T)\,, \tag{9}$$

where the symmetry is that between points and basic open sets given via the elementhood relation. One might compare this observation with the fact, noticed before, that the operator $U \mapsto U^{\lhd}$ is—just as $T \mapsto \overline{T}$—a closure operator.

Constructively, complementation is not a well-behaved operator on subsets. Hence interior and closure, just as openness and closedness, have to be treated as related but separate issues rather than simply defining one through the other. Now membership of the concrete interior reads as

$$x \in \mathring{T} \iff \exists b \ni x \;\; \forall y \in b \;\; (y \in T)\,. \tag{10}$$

Following the same path as from (8) to (9) but now in the reverse direction, one ends up at

$$a \in U^{?} \iff \exists y \in a \;\; \forall b \ni y \; (b \in U), \tag{11}$$

which not surprisingly defines an interior operator $U \mapsto U^{?}$, similar to $T \mapsto \mathring{T}$. Instead of invoking the symmetry between points with basic open sets, to arrive at (11) one may equally have dualised (8) by replacing each occurrence of $\forall$ and $\exists$ by one of $\exists$ and $\forall$, respectively, in the same way in which one may pass from (9) to (10).

A more refined duality becomes necessary when one wishes to distinguish more sharply between membership of a subset and membership of the whole set, as in [52]. Then (8) and (11) have to be reformulated as

$$\begin{aligned} a \in U^{\lhd} &\iff \forall y \in X \;\; (y \in a \Rightarrow \exists b \in A \;\; (y \in b \wedge b \in U))\,, \\ a \in U^{?} &\iff \exists y \in X \;\; (y \in a \wedge \forall b \in A \;\; (y \in b \Rightarrow b \in U))\,, \end{aligned}$$

respectively; whence one needs to replace, in addition, each occurrence of $\Rightarrow$ by one of $\wedge$ and vice versa.

This can easily be justified from every perspective, such as Martin-Löf type theory [36], from which propositions are identified with sets, and proofs with elements. Then $P \Rightarrow Q$ reads as $P \subset Q$, which in turn amounts to $\forall x \in P\ (x \in Q)$. By the common duality between $\exists$ and $\forall$, the latter statement is dual to $\exists x \in P\ (x \in Q)$, and thus to $P \between Q$ or—back to the propositional interpretation—to $P \wedge Q$. (To avoid ending up with $Q \between P$ and $Q \wedge P$, one has to take into account that P plays the role of an index set, as one over which either quantification takes place, whereas Q is relatively arbitrary.)

For all this, it should be clear that the statement $a \mathbin{?} U$—that is, $a \in U^{?}$—is of considerable interest. One of the achievements of the basic picture was to understand it as the intended meaning of a new relation $\ltimes$ between basic opens a and arbitrary opens U of any formal topology whatsoever. The name chosen for it, binary positivity or positivity relation, is motivated by the fact that, for a concrete topological space, the predicate $a \mathbin{?} A$ of basic open sets a is tantamount to a being inhabited, which is nothing but the intended meaning of the unary positivity or positivity predicate evaluated at a.

The following axioms for such a new relation $\ltimes$, which of course are satisfied by its concrete forerunner ? considered above, were first proposed in [51]. Given an arbitrary formal topology with A as the underlying set of basic opens and a covering relation $\lhd$, a *positivity relation* or *binary positivity* is a second relation $a \ltimes U$ between basic opens a and arbitrary opens U. It is required to fulfil the conditions

$$\begin{array}{lccc} \textit{Coreflexivity} & a \ltimes U & \Longrightarrow & a \in U \\ \textit{Cotransitivity} & a \ltimes V \wedge \forall b \in A\ (b \ltimes V \Rightarrow b \in U) & \Longrightarrow & a \ltimes U \end{array}$$

as well as

$$\textit{Compatibility} \quad a \ltimes U \wedge a \lhd V \implies V \ltimes U$$

for all $a \in A$ and $U, V \subset A$ with the notation

$$V \ltimes U \iff \exists b \in A\ (b \in V \wedge b \ltimes U)\,.$$

In other words, the operator $U \mapsto U^{\ltimes}$ on the subsets of A with

$$U^{\ltimes} = \{a \in A : a \ltimes U\}$$

is an *interior operator*, that is,

$$U^{\ltimes} \subset U\,, \quad \text{and} \quad V^{\ltimes} \subset U \implies V^{\ltimes} \subset U^{\ltimes}\,,$$

and it is compatible with the closure operator in the sense that

$$U^{\ltimes} \between V^{\lhd} \implies U^{\ltimes} \between V\,.$$

It is worth pointing out that coreflexivity and cotransitivity of the positivity relation are perfectly dual to reflexivity and transitivity of the covering relation. As with the latter conditions, moreover, the monoid structure does not enter the former ones at all; whence one may define a *basic formal topology* to be simply a set A together with two relations $\lhd$ and $\ltimes$, between elements and subsets of A, which satisfy reflexivity, transitivity, coreflexivity, cotransitivity, and compatibility. When one adds 'down' to these defining conditions of a basic formal topology, one gets the concept of a *balanced formal topology*, which includes as a special case that A be equipped with a monoid structure (see above).

Note furthermore that $\ltimes$ is compatible with $\lhd$ if and only if $a \ltimes U$ is a monotone predicate of $a \in A$ for all $U \subset A$. When one decides to step back from a binary positivity $\ltimes$ to its unary forerunner, and sets

$$\mathrm{Pos}(a) \iff a \ltimes A$$

for $a \in A$ as in [48], then Pos is monotone by the compatibility of $\ltimes$, and satisfies

$$a \ltimes V \implies \mathrm{Pos}(a) \tag{12}$$

for all $a \in A$ and $V \subset A$ by the special case $U = A$ of the cotransitivity of $\ltimes$. (The coreflexivity of $\ltimes$ does not contribute anything to the properties of Pos, as it is trivially satisfied for $U = A$.)

We now return to the case of a commutative ring A. In the case of the concrete Zariski spectrum of A, the relation $a\,?U$ we have considered in (11) reads as

$$\exists\, \mathfrak{p} \in \mathrm{Spec}(A)\ (\mathfrak{p} \in D(a) \wedge \forall\, b \in A\ (\mathfrak{p} \in D(b) \Rightarrow b \in U))\,. \tag{13}$$

An equivalent formulation of (13) is

$$\exists\, \mathfrak{p} \in \mathrm{Spec}(A)\ (a \in A \setminus \mathfrak{p} \subset U)\,, \tag{14}$$

but even if we interpret this as that a belongs to a *prime* coideal contained in U, it still involves points: as we shall see later, the prime filters of A are precisely the formal points of the formal Zariski topology (Proposition 27).

While looking for properties of a relation between a and U which entail that it is a binary positivity, one realises soon that, fortunately, a condition weaker than (14) suffices: namely, that only some *power* coideal lies between a and U. Although this relation still involves some quantification over subsets, its choice is necessary in view of the following observation.

Lemma 18. *Let A be a commutative ring, $\ltimes$ a relation between elements and subsets of A, and $U \subset A$. Then $U^{\ltimes}$ is a power coideal if and only if compatibility holds for this U and all (finite) $V \subset A$.*

Proof. With $a \ltimes U$ in place of pos(a), this is a special instance of Lemma 5; the particular case $a = 0$ and $V = \emptyset$ of compatibility ensures that $U^{\ltimes} \subset \neg\{0\}$. □

As consequences of the definitions of $I(U)$ and $R(U)$, we furthermore notice that

$$I(U) = \bigcap \{I \subset A : I \text{ ideal}, I \supset U\}\,, \tag{15}$$

$$R(U) = \bigcap \{R \subset A : R \text{ radical ideal}, R \supset U\}\,; \tag{16}$$

so $I(U)$ and $R(U)$ are the smallest ideal and radical ideal, respectively, that contain U.

To avoid any vicious circle, one must not define $I(U)$ and $R(U)$ through (15) and (16), because then the *definiendum* would occur, as one of the (radical) ideals containing U, already within the *definiens*, the intersection of all those (radical) ideals. Nothing hinders us, however, from asserting and proving (15) and (16) as immediate consequences of the comparatively descriptive definitions of $I(U)$ and $R(U)$ that have been given before with (2) and (3).

Dualising (15) and (16), we provisionally set

$$C(U) = \bigcup \{C \subset A : C \text{ coideal}, C \subset U\}, \tag{17}$$

$$P(U) = \bigcup \{P \subset A : P \text{ power coideal}, P \subset U\}, \tag{18}$$

which are the largest coideal and power coideal, respectively, that are contained in U. Equally provisionally, we define

$$a \ltimes U \iff a \in P(U) \tag{19}$$

for all $a \in A$ and $U \subset A$.

The provisional character of these definitions is only because of the possible suspicion, with which we do not completely agree (see below), that they might not be fully predicative either. As we will justify them in a moment anyway, by a coinductive generation which, in addition, has the following proposition as a by-product, one may accept these definitions at least as a *façon de parler.*

Proposition 19. *Let A be a commutative ring. Then $\ltimes$ is a positivity relation: that is, it is coreflexive, cotransitive, and compatible with $\lhd$. Moreover, P is the largest operator on the subsets of A that is compatible with R, and for which $P(U) \subset U$ for all $U \subset A$.*

Proof. By definition, $P(U) \subset U$, and if $P(U) \subset V$, then $P(U) \subset P(V)$, which is to say that P is an interior operator. By Lemma 18, P is compatible with R. On the other hand, if Q is an operator on the subsets of A that is compatible with R, then Q is a power coideal (Lemma 18). If, moreover, $Q(U) \subset U$, then $Q(U) \subset P(U)$. $\square$

In view of

$$R(U) = \left\{a \in A : M(a) \between I(U)\right\}$$

with

$$M(a) = \left\{a^n : n \in \mathbb{N}_0\right\},$$

one might recall the dualities peculiar to the basic picture and think of

$$Q(U) = \{a \in A : M(a) \subset C(U)\}$$

as another candidate for an interior operator. However, if Q is compatible with R, then $Q(U) \subset P(U)$, so that $Q(U) = P(U)$ because $P(U) \subset Q(U)$: if $a \in P(U)$, then $M(a) \subset P(U)$.

Unlike the case of (15) and (16), we hold it is less likely that one would get caught in any trap of impredicativity when we use (17) and (18) as definitions: to establish any given $a \in A$ as an element of the largest (power) coideal contained in U, one has to find an arbitrary (power) coideal that lies between a and U, no matter whether this eventually turns out to coincide with the actually largest one.

One may admit that to *introduce* membership of $C(U)$ and $P(U)$ seems harmless, but suspect that to *eliminate* membership causes doubts: given $a \in P(U)$, say, how can one find a power coideal P with $a \in P \subset U$ without having to check, at least in the worst case, *all* the power coideals of A? A possible argument against the latter objection is that an assertion like $a \in P(U)$ should anyway be understood, at least tacitly, as the presence of such a witness P.

To avoid entering this discussion more deeply, and to do away with further reservations, we will next (re-)define $P(U)$ by way of a coinductive generation, which allegedly looks safe from the predicative standpoint. Before so doing, we notice that the case is as with the interior $\mathring{T}$ versus the closure $\overline{T}$ of each subset T of a concrete topological space, whose interaction gave rise to the basic picture (see above). To define $\overline{T}$ 'from above', as the smallest closed superset of T, definitely involves self-reference; whence this is better done by way of (9). On the other hand, it seems less problematic to define $\mathring{T}$ 'from below', as the largest open subset of T; in fact this is nothing but (10).

6.1. Simultaneous generation

Unlike the case of I and R, it is not plain at all how C and P could intrinsically be described in terms of the algebraic structure of A. We are nonetheless able to modify the canonical inductive generation which $\lhd$ admits as a Stone covering [16] so that it carries over to a coinductive generation of $\ltimes$. By so doing, we provide a *simultaneous* generation of $\lhd$ and $\ltimes$ as it has been proposed by Martin-Löf and Sambin [49][30]; whence in the present case there is no need to use the more general approach put forward by Valentini [60] by which $\lhd$ and $\ltimes$ can be (co)inductively generated *independently* from each other. We refer to [9] for a detailed treatment of induction and coinduction within type theory.

To recall briefly the general idea of an inductive generation, we consider the original case, the set $\mathbb{N}$ of natural numbers. This is inductively generated by the introduction rules $1 \in \mathbb{N}$ and $n \in \mathbb{N} \Rightarrow n + 1 \in \mathbb{N}$. In other words, $\mathbb{N}$ is the smallest set satisfying these rules or, equivalently, it satisfies the elimination rule—perhaps more widely known as the principle of complete induction (*sic!*) for natural numbers—which says that if S is a set such that $1 \in S$ and $n \in S \Rightarrow n + 1 \in S$, then $\mathbb{N} \subset S$.

When it comes to inductively generate covering relations, one might first think of reflexivity and transitivity as suitable introduction rules. The latter one, however, immediately causes doubts from a predicative perspective: the antecedent $a \lhd U \wedge U \lhd V$ requires the existence of an intermediate arbitrary open U that does not occur in the consequent $a \lhd V$, and thus to quantify over general subsets U. The case is as with proofs involving *modus ponens*: when one wishes to follow inductive generations containing occurrences of transitivity in the backwards direction, then one may encounter an instance of $a \lhd V$ that possibly stems from $a \lhd U \wedge U \lhd V$ for a yet unknown intermediate term U, and in the worst case one may be bound to check *all* the subsets to find the right one.

A way out of this situation was proposed in [16], which we now summarise. Let A be an arbitrary set, and assume that we are given a family of index sets $J(a)$ with $a \in A$, and a family of subsets $D(a, j)$ of A with $a \in A$ and $j \in J(a)$. The intended meaning of all this is that, for each $a \in A$, every $j \in J(a)$ is a name for a subset $D(a, j)$ that covers a; so that the relation $<$ with

[30] The author wishes to thank Giovanni Sambin and Per Martin-Löf for having insisted on the viability of this road also in the case of formal Zariski topology.

$$a < U \iff \exists j \in J(a)\ (D(a, j) \subset U)$$

for $a \in A$ and $U \subset A$ is a first candidate for a covering relation.

As $<$ need not satisfy reflexivity and transitivity, to arrive at a proper covering one has to 'close' $<$ with respect to these conditions. To this end, one defines $\lhd$ as the relation inductively generated by the introduction rules

$$\begin{array}{llcl} \textit{Reflexivity} & a \in U & \Longrightarrow & a \lhd U \\ \textit{Infinity} & j \in J(a) \wedge D(a, j) \lhd U & \Longrightarrow & a \lhd U \end{array}$$

for $a \in A$ and $U \subset A$. In other words, $\lhd$ is the narrowest relation satisfying reflexivity and infinity: it enjoys the elimination rule which says that if $\lhd'$ is any relation between elements and subsets of A such that reflexivity and infinity hold with $\lhd'$ in place of $\lhd$, then $\lhd$ is already contained in $\lhd'$. Moreover, $\lhd$ is not only reflexive and transitive, but also contains $<$; indeed it is the narrowest relation with all these features. In particular, if $<$ happens to be a covering relation, then $\lhd$ coincides with $<$.

In the case of a Stone covering $\lhd$, if

$$J(a) = \{U_0 \subset A : U_0 \text{ finite}, a \lhd U_0\} \quad (a \in A)$$

is a family of sets, then

$$D(a, U_0) = U_0 \quad (a \in A,\ U_0 \in J(a))$$

is a family of subsets of A. With these data, every Stone covering $\lhd$ is inductively generated [16]. As $<$ coincides with $\lhd$ in any such case, at first glance there seems to be no real need of doing inductive generation for Stone coverings. However, the method of (co)inductive definition immediately becomes useful as soon as one aims at equally providing positivity relations.

Indeed, in [49] one defines $\ltimes$ as the relation that is coinductively generated by the cointroduction[31] rules

$$\begin{array}{llcl} \textit{Coreflexivity} & a \ltimes U & \Longrightarrow & a \in U \\ \textit{Coinfinity} & j \in J(a) \wedge a \ltimes U & \Longrightarrow & D(a, j) \ltimes U \end{array}$$

for $a \in A$ and $U \subset A$. In other words, $\ltimes$ is the widest relation satisfying coreflexivity and coinfinity: it enjoys the coelimination rule which say that if $\ltimes'$ is any relation between elements and subsets of A such that coreflexivity and coinfinity hold with $\ltimes'$ in place of $\ltimes$, then $\ltimes'$ is already contained in $\ltimes$.

This $\ltimes$ is coreflexive and cotransitive; moreover, if $\lhd$ and $\ltimes$ are generated inductively and coinductively, respectively, with *the same* families $J(a)$ and $D(a, j)$, then $\ltimes$ is automatically compatible with $\lhd$. In this vein, we say that $\lhd$ and $\ltimes$ are *simultaneously generated* whenever they are generated inductively and coinductively, respectively, for an appropriate *common* choice of the families $J(a)$ and $D(a, j)$.

The following has been stated in [49], and a proof can be found in [37].

31 Without the prefix 'co', which in this context we have seen in [9], one ought to switch the names 'elimination' and 'introduction' when passing from inductive to coinductive generation: they would match their meaning only then.

Proposition 20. *If $\lhd$ and $\ltimes$ are simultaneously generated relations on a set A, then A together with $\lhd$ and $\ltimes$ is a basic formal topology.*

Note that if $\lhd$ was already given, if it is a Stone covering, and if $J(a)$ and $D(a, j)$ are as above for any Stone covering, then (co)infinity is nothing but (co)transitivity for finite intermediate terms.

To return to the case of the formal Zariski topology, let A be a commutative ring with the covering $\lhd$ defined in Section 4. We choose $J(a)$ and $D(a, j)$ as for any Stone covering; in other words, we set

$$J(a) = \{U_0 \subset A : U_0 \text{ finite}, a \in R(U_0)\} \quad (a \in A),$$

$$D(a, U_0) = U_0 \quad (a \in A,\ U_0 \in J(a)).$$

With this choice of the families $J(a)$ and $D(a, j)$, we now redefine $\lhd$ and $\ltimes$ as the relations simultaneously generated by reflexivity and infinity as well as by coreflexivity and coinfinity.[32]

The following unwinding of infinity and coinfinity helps to see that we thus get nothing but the relations $\lhd$ and $\ltimes$ which we have already considered before. To start with, observe that infinity reads as

$$U_0 \subset U^{\lhd} \implies R(U_0) \subset U^{\lhd} \quad (U_0 \subset A,\ U_0 \text{ finite}); \tag{20}$$

whence the narrowest relation $\lhd$ satisfying infinity and reflexivity is nothing but the covering relation $\lhd$ with $U^{\lhd} = R(U)$ as the smallest radical ideal that contains U (compare Lemma 2). Dually, the essence of coinfinity is

$$R(U_0) \between U^{\ltimes} \implies U_0 \between U^{\ltimes} \quad (U_0 \subset A,\ U_0 \text{ finite}), \tag{21}$$

so that the widest relation satisfying coinfinity and coreflexivity coincides with the positivity relation $\ltimes$ that we have provisionally defined earlier on: with $U^{\ltimes} = P(U)$ as the largest power coideal that is contained in U (compare Lemma 3).

In view of Proposition 20, we have the following.

Corollary 21. *For every commutative ring A, the relations $\lhd$ and $\ltimes$ are simultaneously generated; whence the formal Zariski topology of A is a basic formal topology.*

As a by-product we regain Proposition 19, and parts of Proposition 4.

32 As we have done in [54], one may impose the extra rules

$$\textit{Zero} \quad a = 0 \implies a \lhd U \qquad \textit{Cozero} \quad a \ltimes U \implies a \neq 0$$

when simultaneously generating $\lhd$ and $\ltimes$. In view of $\emptyset \in J(0)$, 'zero' is redundant anyway. 'Cozero', on the other hand, follows from compatibility whenever $\neq$ stands for the *denial* inequality (compare Lemma 18), in which case there is no need of requiring 'cozero' to ensure that $U^{\ltimes}$ is a (power) coideal.
If, however, one wishes to achieve 'cozero' for an *arbitrary* inequality (for instance, if—as we did in [54]—one decides to require $S \subset \sim \{0\}$ rather than $S \subset \neg\{0\}$ from every coideal), then one needs to add 'cozero' to the rules for simultaneous generation. As Jesper Carlström kindly pointed out to us, the drawbacks of this move are that one must modify the technique of simultaneous generation, and that it produces a covering and a positivity relation which are possibly wider and narrower, respectively, than $\lhd$ and $\ltimes$.

6.2. *The derived predicate*

We define the predicate Pos attached to a commutative ring A by setting

$$\mathrm{Pos}(a) \iff a \ltimes A$$

for $a \in A$, so that

$$P(A) = \{a \in A : \mathrm{Pos}(a)\}.$$

The compatibility of $\ltimes$ automatically yields that Pos is monotone.

We now assume—for the rest of Section 6—that $\neq$ be the denial inequality on the commutative ring A under consideration. Since then $\mathrm{Pos}_0(a)$ coincides with $\neg(a \lhd \emptyset)$, we have

$$\mathrm{Pos}(a) \implies \mathrm{Pos}_0(a)$$

for every $a \in A$ by the monotonicity of Pos; more generally,

$$\begin{array}{ccc} C(A) & \subset & C_0(A) \\ \cup & & \cup \\ P(A) & \subset & P_0(A) \end{array} \tag{22}$$

where

$$C_0(A) = \{a \in A : a \neq 0\}, \quad P_0(A) = \{a \in A : \mathrm{Pos}_0(a)\}.$$

In particular, every coideal (respectively, every power coideal) lies inside $C_0(A)$ (respectively, inside $P_0(A)$).

By definition, $C(A) = C_0(A)$ if and only if $C_0(A)$ is a coideal, and $P(A) = P_0(A)$ if and only if $P_0(A)$ is a power coideal. Since $\neq$ is a ring inequality, the additive property of a coideal is the only missing condition for $C_0(A)$ to be a coideal and for $P_0(A)$ to be a power coideal, which in the case of $C_0(A)$ amounts to $\neq$ being cotransitive.

Moreover, $P_0(A) = C_0(A)$ precisely when A is reduced. So if A is reduced and $\neq$ is cotransitive, then $P_0(A)$ is a power coideal and thus $P(A) = P_0(A)$; whence all the subsets in (22) are equal.

Since Pos is monotone, it coincides with Pos_0 only if the latter is also monotone. According to the coinductive generation of $\ltimes$, this necessary condition is also a sufficient one: Pos is the widest monotone predicate on A with $P(A) \subset C_0(A)$. Lemma 5 provides the only missing link in the following result.

Proposition 22. *Let A be a commutative ring with the denial inequality $\neq$. Then the following items are equivalent:*

1. Pos_0 *is monotone.*
2. $P_0(A)$ *is a power coideal.*
3. $P(A) = P_0(A)$.
4. Pos *coincides with* Pos_0.

In view of Propositions 7 and 10, we also have the following.

Corollary 23. *If A is quasireduced and the denial inequality $\neq$ is cotransitive, then* Pos *coincides with* Pos_0.

Corollary 24. *LLPO is equivalent to* Pos *coinciding with* Pos_0 *for every discrete commutative ring.*

The next result indicates that, constructively, the openness of Pos is not always a *desideratum*.

Corollary 25. *LPO follows from the statement that* Pos *is open for every discrete commutative ring A.*

Proof. Let $A = D$ be the discrete ring given in the proof of Proposition 8. As Pos_0 is monotone for this ring (see the proof of Corollary 9), it coincides with Pos (Proposition 22). So if Pos is open, then so is Pos_0, and Proposition 14 applies. □

In particular, if the derived positivity predicate Pos is open for every basic formal topology with a Stone covering, then LPO holds. So one has to be careful with 'forcing' openness as proposed in [49], by 'adding it at will' to the properties of such a Pos: that is, by deliberately adjoining this condition to the other ones. We refer to Proposition 15 and Proposition 16 for how to relate WLPO and MP in an analogous way to 'proofs by cases' and '*ex falso quodlibet*', respectively, for Pos.

For all this, we believe to have made a good choice of the positivity relation $\ltimes$ and the interior operator P for the formal Zariski topology of a commutative ring A.

7. Are there enough points?

The notion of a formal point, with which a formal topology—as every truly point-free setting—can only be decorated afterwards, is guided by the intuition that a formal point consists of the indices of the basic open sets which belong to a neighbourhood filter of an imagined concrete point. Unlike the case of ordinary topological spaces, formal points are by no means constitutive for formal topologies, for which those indices, the basic opens, are the primitive objects.

Given a formal topology with underlying set A and covering relation $\lhd$, a *formal point* is a subset ξ of A with the following properties: first, ξ is inhabited; secondly, ξ satisfies

$$a \in \xi \wedge b \in \xi \implies \xi \between a \downarrow b \tag{23}$$

for all $a, b \in A$; thirdly, ξ is monotone in the sense that

$$a \in \xi \wedge a \lhd U \implies \xi \between U \tag{24}$$

for all $a \in A$ and $U \subset A$. We have already encountered the latter condition in the case of the positivity predicate.[33]

[33] It is because of the different intuitions connected with a formal point and a positivity predicate that one speaks of the former as a subset and of the latter as a predicate, although subsets can—and perhaps should—be understood as in type-theoretic contexts [52]: as predicates on the ambient set.

On the level of the frame $\mathrm{Sat}\,(A)$ of formal opens, a formal point is nothing but a completely prime filter [47].[34] As the latter is an adequate notion of a point in the theory of locales, the observations recalled in the following paragraph (for which we refer to [28, II.1.3–7]) are completely analogous to the corresponding ones for locales, but likewise require some impredicative reasoning.

The *collection* $\mathrm{Pt}\,(A)$ *of formal points* can be endowed with the *extensional topology* of which

$$\{\xi \in \mathrm{Pt}\,(A) : \xi \in a\} \qquad (a \in A)$$

is a basis of open sets, and with which $\mathrm{Pt}\,(A)$ is a sober topological space. If A itself is a basis of open sets of an already given topological space X, then the canonical continuous mapping

$$X \to \mathrm{Pt}\,(A)\,,\; x \mapsto \{a \in A : x \in a\}$$

is a homeomorphism precisely when X is sober.

When A comes with a monoid structure as in [47], then (23) is given its stronger form

$$a \in \xi \wedge b \in \xi \implies ab \in \xi \tag{25}$$

for all $a \in A$ and $U \subset A$, and every monotone ξ is inhabited if and only if $1 \in \xi$. In particular, ξ being a multiplicative subset is part of the definition of ξ being a formal point.

In the presence of a positivity predicate pos on A, a formal point ξ is required to satisfy the additional condition

$$a \in \xi \implies \mathrm{pos}(a) \tag{26}$$

for all $a \in A$. The intuition standing behind (26) is that if a represents a basic open set contained in a neighbourhood filter—the one represented by ξ—of a certain point, then a is inhabited by this point. Note that (26) is a consequence of (24)) whenever pos is open and monotone [41].

In the case of a basic formal topology with positivity relation $\ltimes$, one even expects every formal point ξ to fulfil the condition dual to ξ being monotone [51]: that is,

$$a \in \xi \wedge \xi \subset U \implies a \ltimes U \tag{27}$$

for all $a \in A$ and $U \subset A$. When one steps back from a binary positivity $\ltimes$ to the unary one with $\mathrm{Pos}(a)$ as $a \ltimes A$, then (27) collapses to (26) for Pos.

A formal topology is said to be *spatial* or *to have enough points* if there are sufficiently many formal points to recover the covering [47,21,18]: that is,

$$\forall \xi \;\big(a \in \xi \Rightarrow \xi \between U\big) \implies a \lhd U \tag{28}$$

for all $a \in A$ and $U \subset A$. Here ξ varies over the formal points whose defining properties depend on the context, and thus always need to be specified. Note that the converse of (28)

[34] Although the notions of (prime) filter and (prime) ideal in a lattice are analogous to their ring-theoretic forerunners, we do not to explain the latter, which—as lattice-theoretic concepts in general—are somewhat secondary to the present setting. We refer instead to [28, I.2.1–2].

is nothing but (24): the latter says that if $a \lhd U$ and ξ is a formal point with $a \in \xi$, then $\xi \between U$.

As an instance of a universal quantification over subsets, even over point-like items, (28) causes doubts from a predicative perspective. It actually is a relatively strong principle, as the following adaptation of 'every spatial locale is open' [29, p. 99] shows.

Proposition 26. *If a formal topology has enough points satisfying* (26) *for an arbitrary predicate* pos *of basic opens, then* pos *is open.*

Proof. We verify positivity for pos. To this end, let $a \in A$ and $U \subset A$, and assume that $\mathrm{pos}\,(a) \Rightarrow a \lhd U$. If ξ is a formal point satisfying (26), then $a \in \xi$ implies $a \lhd U$ by our assumption. Hence, for any such ξ, if $a \in \xi$, then $\xi \between U$ by (24). In other words, the antecedent of (28) holds, so that $a \lhd U$. □

In this result, pos neither has to be open, which it a posteriori is, nor monotone. There is furthermore no need to assume that formal points satisfy (23) or even (25), let alone that a monoid structure is given on A.

We now return to the formal Zariski topology of a commutative ring A. Its formal points have a neat algebraic characterisation, which coincides with the one given in locale theory [28, V.3.2]. All this is little surprising when one takes into account that the points of the concrete topological space $\mathrm{Spec}\,(A)$ are the prime ideals of A whose complements are—classically—the prime filters of A.

Proposition 27. *Let A be a commutative ring. The formal points of the formal Zariski topology of A are precisely the prime filters of A. More specifically, the following items are equivalent for each subset ξ of A:*

1. *ξ is a prime filter.*
2. *$1 \in \xi$, and ξ satisfies* (24) *and* (25).
3. *$1 \in \xi$, and ξ satisfies* (24), (25), *and* (27).
4. *$1 \in \xi$, and ξ satisfies* (24), (25), *and* (26) *with* $\mathrm{Pos}\,(a)$ *in place of* $\mathrm{pos}\,(a)$.
5. *$1 \in \xi$, and ξ satisfies* (24), (25), *and* (26) *with* $\neg\,(a \lhd \emptyset)$ *in place of* $\mathrm{pos}\,(a)$.
6. *$1 \in \xi$, and ξ satisfies* (24), (25), *and* (26) *with* $\neg\,(a = 0)$ *in place of* $\mathrm{pos}\,(a)$.

Proof. Notice first that ξ is a multiplicative subset precisely when it contains 1 and enjoys property (25). Secondly, condition (24) amounts to $a \in \xi$ being a monotone property of a, which by Lemma 5 is equivalent to ξ being a power coideal. Since a prime filter is a (power) coideal that, in addition, is a multiplicative subset, the first and the second item are equivalent. Similarly, if ξ is a prime filter, then ξ is a power coideal, so that (27) is fulfilled according to the definition of $\ltimes$. Observe next that (27) implies (26) for $\mathrm{Pos}\,(a)$, and thus also for $\neg\,(a \lhd \emptyset)$, since the latter predicate contains the former. Clearly, the fifth item implies the sixth, which in turn implies the second. □

Since the Zariski frame of A, the frame of radical ideals of A, is perfectly coherent, every prime filter in this frame is complete a priori; moreover, the Zariski frame is nothing but the frame $\mathrm{Sat}\,(A)$ of formal opens of the formal Zariski topology of A. Proposition 27 therefore implies that the prime filters of A as a ring are precisely the prime filters of the Zariski frame of A. Like the analogous fact for prime ideals [14], this observation elucidates once more the close relation between the ring structure of A and its lattice-theoretic counterpart.

Moreover, the classical Zariski spectrum Spec (A) is a sober topological space; whence the canonical mapping Spec $(A) \to$ Pt (A) is a homeomorphism. It maps each prime ideal $\mathfrak{p}$ to its complement $A \setminus \mathfrak{p}$, for the latter equals $\{a \in A : \mathfrak{p} \in D(a)\}$.

In view of Propositions 26 and 27, we cannot expect a constructive proof that the formal Zariski topology has enough points: this is too strong an assumption even for discrete rings (see Proposition 14 or Corollary 25).

Corollary 28. *LPO follows from the assumption that, for every discrete commutative ring A, the formal Zariski topology of A has enough points.*

As in the case of Proposition 14, to arrive at LPO it suffices to assume 'enough points' for the ring D of the proof of Proposition 8, and thus for every discrete ring of the form $\mathbb{Z}[t]$. In view of Proposition 27, we can state Corollary 28 as it stands, without specifying which—if any—of the available concepts of positivity enters the definition of a formal point. (This equally holds for $\mathrm{Pos}_0(a)$, since it is equivalent to $\neg(a \lhd \emptyset)$ whenever $\neq$ is the denial inequality.) In other words, the choice of a notion of positivity is completely irrelevant for the constructive lack of points for the formal Zariski topology.

Acknowledgements

Suggestions by Douglas Bridges, Giovanni Curi, and Silvia Gebellato were useful in bringing the forerunner [54] of this article into its final form. Comments by Jesper Carlström, Henri Lombardi, and Steve Vickers helped to improve it later. Last but not least, the author is grateful to Laura Crosilla for taking on also his portion of the joint organisation of a workshop while [54] was written.

References

[1] P. Aczel, N. Gambino, Collection principles in dependent type theory, in: P. Callaghan, Z. Luo, J. McKinna, R. Pollack (Eds.), Types for Proofs and Programs (Proc. Internat. Workshop TYPES 2000, Durham, United Kingdom), in: Lect. Notes Comput. Sci., vol. 2277, Springer, Berlin, Heidelberg, 2002, pp. 1–23.

[2] B. Banaschewski, The power of the ultrafilter theorem, J. London Math. Soc. 27 (1983) 193–202.

[3] G. Battilotti, G. Sambin, Pretopologies and a uniform presentation of sup-lattices, quantales and frames (forthcoming).

[4] J.L. Bell, Zorn's lemma and complete Boolean algebras in intuitionistic type theories, J. Symbolic Logic 62 (1997) 1265–1279.

[5] D.S. Bridges, Constructive mathematics: a foundation for computable analysis, Theoret. Comput. Sci. 219 (1999) 95–109.

[6] D.S. Bridges, Prime and maximal ideals in the constructive theory of rings with inequality, Commun. Algebra 29 (2001) 2787–2803.

[7] D. Bridges, F. Richman, Varieties of Constructive Mathematics, in: London Math. Soc. Lect. Notes, vol. 97, Cambridge University Press, Cambridge, 1987.

[8] D. Bridges, F. Richman, P. Schuster, A weak countable choice principle, Proc. Amer. Math. Soc. 128 (2000) 2749–2752.

[9] V. Capretta, Abstraction and computation. Type theory, algebraic structures, and recursive functions. Doctoral Dissertation, Catholic University of Nijmegen, 2002.

[10] J. Carlström, Subsets, quotients and partial functions in Martin-Löf's type theory, in: H. Geuvers, F. Wiedijk (Eds.), Types for Proofs and Programs (Proc. Internat. Workshop TYPES 2002, Berg en Dal, The Netherlands), in: Lect. Notes Comput. Sci., vol. 2646, Springer, Berlin, Heidelberg, 2003.
[11] J. Cederquist, An implementation of the Heine–Borel covering theorem in type theory, in: E. Gimnez, C. Paulin-Mohring (Eds.), Types for Proofs and Programs (Proc. Internat. Workshop TYPES 1996, Aussois, France), in: Lect. Notes Comput. Sci., vol. 1512, Springer, Berlin, Heidelberg, 1998, pp. 46–65.
[12] J. Cederquist, Th. Coquand, Entailment relations and distributive lattices, in: S. Buss, P. Hájek, P. Pudlák (Eds.), Logic Colloquium 1998 (Proc. Prague, Czech Republic), in: Lect. Notes Logic, vol. 13, Assoc. Symb. Logic, Urbana, Ill, 2000, pp. 127–139.
[13] J. Cederquist, S. Negri, A constructive proof of the Heine–Borel covering theorem for formal reals, in: S. Berardi, M. Coppo (Eds.), Types for Proofs and Programs (Proc. Internat. Workshop TYPES 1995, Torino, Italy), in: Lect. Notes Comput. Sci., vol. 1158, Springer, Berlin, 1996, pp. 62–75.
[14] Th. Coquand, H. Lombardi, Hidden constructions in abstract algebra (3). Krull dimension of distributive lattices and commutative rings, in: M. Fontana, S.-E. Kabbaj, S. Wiegand (Eds.), Commutative Ring Theory and Applications, in: Lect. Notes Pure Appl. Math., vol. 131, Dekker, New York, 2002, pp. 477–499.
[15] Th. Coquand, S. Sadocco, G. Sambin, J. Smith, Formal topologies on the set of first-order formulae, J. Symbolic Logic 65 (2000) 1183–1192.
[16] Th. Coquand, G. Sambin, J. Smith, S. Valentini, Inductive generation of formal topologies, Ann. Pure Appl. Logic 124 (2003) 71–106.
[17] D. Cox, J. Little, D. O'Shea, Ideals, Varieties, and Algorithms, 2nd ed., Springer, Berlin, Heidelberg, New York, 1997.
[18] G. Curi, Formal topology as expression of contemporary mathematics, University of Siena, 2003.
[19] R. Diaconescu, Axiom of choice and complementation, Proc. Amer. Math. Soc. 51 (1975) 176–178.
[20] M.P. Fourman, R.J. Grayson, Formal Spaces, in: A.S. Troelstra, D. van Dalen (Eds.), The L.E.J. Brouwer Centenary Symposion (Proc. 1981 Conf. Noordwijkerhout, The Netherlands), in: Studies Logic Found. Math., vol. 110, North Holland, Amsterdam, 1982, pp. 107–122.
[21] N. Gambino, Sheaf interpretations for generalised predicative intuitionistic systems, Doctoral Dissertation, University of Manchester, 2002.
[22] S. Gebellato, G. Sambin, The essence of continuity, in: G. Sambin, S. Gebellato, P. Martin-Löf, V. Capretta (Eds.), The basic picture, University of Padua, 2003 (preprint).
[23] S. Gebellato, G. Sambin, Pointfree continuity and convergence. In the same preprint collection as [22].
[24] N.D. Goodman, J. Myhill, Choice implies excluded middle, Z. Math. Logik Grundlag. Math. 23 (1978) 461.
[25] R. Hartshorne, Algebraic Geometry, in: Graduate Texts Math., vol. 52, Springer, New York, 1977.
[26] M. Hochster, Prime ideal structure in commutative rings, Trans. Amer. Math. Soc. 142 (1969) 43–60.
[27] P.T. Johnstone, Rings, fields, and spectra, J. Algebra 49 (1977) 238–260.
[28] P.T. Johnstone, Stone Spaces, in: Cambridge Studies Adv. Math., vol. 3, Cambridge University Press, Cambridge, 1982.
[29] P.T. Johnstone, Open locales and exponentiation, Contemp. Math. 30 (1984) 84–116.
[30] A. Joyal, Les théorèmes de Chevalley–Tarski et remarques sur l'algèbre constructive, Cahiers Topologic Géom. Differentielle 16 (1976) 256–258.
[31] H. Lombardi, Une introduction aux mathématiques constructives, University of Franche-Comté, 1999, p. 89.
[32] H. Lombardi, C. Quitté, Constructions cachées en algèbre abstraite (2). Le principe local–global, in: M. Fontana, S.-E. Kabbaj, S. Wiegand (Eds.), Commutative Ring Theory and Applications, in: Lect. Notes Pure Appl. Math., vol. 131, Dekker, New York, 2002, pp. 461–476.
[33] S. MacLane, I. Moerdijk, Sheaves in Geometry and Logic. A First Introduction to Topos Theory, Springer, New York, 1992.
[34] M.E. Maietti, About effective quotients in constructive type theory, in: Th. Altenkirch, W. Naraschewski, B. Reus (Eds.), Types for Proofs and Programs (Proc. Internat. Workshop TYPES '98, Irsee, Germany), in: Lect. Notes Comput. Sci., vol. 1657, Berlin and Heidelberg, Springer, 1999, pp. 164–178.
[35] M.E. Maietti, S. Valentini, Can you add power-sets to Martin-Löf intuitionistic set theory? Math. Logic Quart. 45 (1999) 521–532.
[36] P. Martin-Löf, Intuitionistic Type Theory. Notes by G. Sambin of a series of lectures given in Padua, June 1980, in: Studies Proof Theory, vol. 1, Bibliopolis, Naples, 1984.

[37] P. Martin-Löf, G. Sambin, Generating positivity by coinduction. In the same preprint collection as [22].
[38] R. Mines, F. Richman, W. Ruitenburg, A Course in Constructive Algebra, Springer, New York, 1987.
[39] C. Mulvey, Intuitionistic algebra and representations of rings, Mem. Amer. Math. Soc. 148 (1974) 3–57.
[40] S. Negri, Stone bases, alias the constructive content of Stone representation, in: A. Ursini, P. Aglianó (Eds.), Logic and Algebra (Proc. Conf. *in memoriam* Roberto Magari, Pontignano, Siena, Italy, 1994), Dekker, New York, 1996, pp. 617–636.
[41] S. Negri, Continuous domains as formal spaces, Math. Struct. Comput. Sci. 12 (2002) 19–52.
[42] J. Neukirch, Algebraic Number Theory, in: Grundl. Math. Wiss., vol. 322, Springer, Berlin, 1999.
[43] B. Nordström, K. Petersson, J. Smith, Programming in Martin-Löf's Type Theory, Oxford University Press, Oxford, 1990.
[44] H. Persson, An application of the constructive spectrum of a ring, in: H. Persson, Type Theory and the Integrated Logic of Programs, Doctoral Thesis, Department of Computing Sciences, Chalmers University of Technology and Gothenburg University, 1999.
[45] M. Pohst, H. Zassenhaus, Algorithmic Algebraic Number Theory, in: Encycl. Math. Appl., vol. 30, Cambridge University Press, Cambridge, 1989.
[46] W. Ruitenburg, Intuitionistic algebra, theory and sheaf models, Doctoral Dissertation, University of Utrecht, 1982.
[47] G. Sambin, Intuitionistic formal spaces—a first communication, in: D. Skordev (Ed.), Mathematical Logic and its Applications (Conf. Proc., Druzhba, Bulgaria, 1986), Plenum, New York, London, 1987, pp. 187–204.
[48] G. Sambin, Formal topology and domains, Electron. Notes Theoret. Comput. Sci. 35 (2000) 14.
[49] G. Sambin, Some points in formal topology, Theoret. Comput. Sci. 305 (2003) 347–408.
[50] G. Sambin, The basic picture, a structure for topology. In the same preprint collection as [22].
[51] G. Sambin, S. Gebellato, A preview of the basic picture: a new perspective on formal topology, in: Th. Altenkirch, W. Naraschewski, B. Reus (Eds.), Types for Proofs and Programs (Proc. Internat. Workshop TYPES '98 Kloster Irsee, Germany), in: Lect. Notes Comput. Sci., vol. 1657, Springer, Berlin, 1999, pp. 194–207.
[52] G. Sambin, S. Valentini, Building up a toolbox for Martin-Löf's type theory: subset theory, in: G. Sambin, J. Smith (Eds.), Twenty-five Years of Constructive Type Theory (Congress Proc., Venice, Italy, 1995), in: Oxford Logic Guides, vol. 36, Oxford University Press, Oxford, 1998, pp. 221–244.
[53] G. Sambin, S. Valentini, P. Virgili, Constructive domain theory as a branch of intuitionistic pointfree topology, Theoret. Comput. Sci. 159 (1996) 319–341.
[54] P.M. Schuster, Spectra and Sheaves in Formal Topology, Habilitationsschrift, Universität München, 2003.
[55] P.M. Schuster, The Zariski spectrum as a formal geometry (forthcoming).
[56] I. Sigstam, Formal spaces and their effective presentations, Arch. Math. Logic 34 (1995) 211–246.
[57] H. Simmons, Reticulated rings, J. Algebra 66 (1980) 169–192.
[58] M. Tierney, On the spectrum of a ringed topos, in: A. Heller, M. Tierney (Eds.), Algebra, Topology, and Category Theory. A Collection of Papers in Honor of Samuel Eilenberg, Academic Press, New York, 1976, pp. 189–210.
[59] A.S. Troelstra, D. van Dalen, Constructivism in Mathematics. An Introduction. Two volumes, Studies Logic Found. Math., vols. 121–123, North Holland, Amsterdam, 1988.
[60] S. Valentini, The problem of the formalization of constructive topology, Arch. Math. Logic 44 (2005) 115–129.
[61] S. Vickers, Topology via Logic, Cambridge Tracts Theoret. Comput. Sci., vol. 5, Cambridge University Press, Cambridge, 1989.